[IN]SECURE

OPEN. INFORMATIVE. TO THE POINT. Issue 20 - March 2009

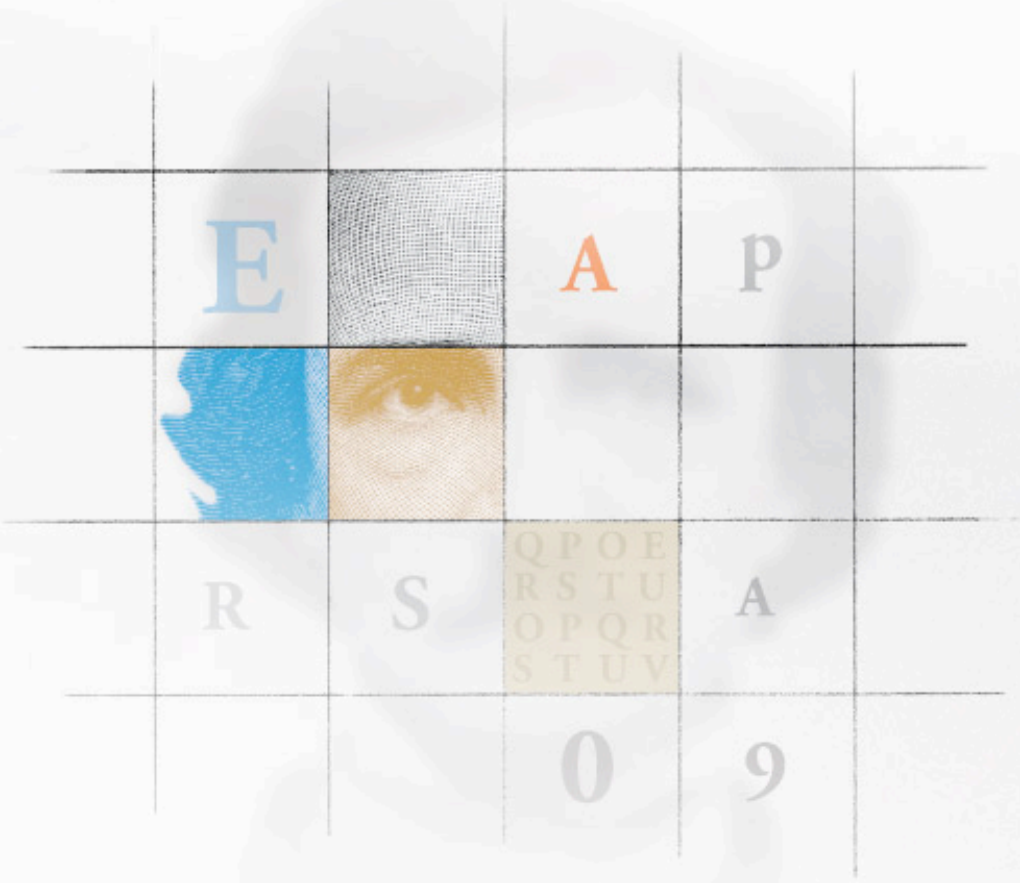
NETWORK DISCOVERY MECHANISMS
THE (IN)SECURITY OF MAC OS X
THE CHINESE UNDERGROUND

RSA® CONFERENCE

WHERE THE WORLD **TALKS SECURITY**

When the next security threat hits, be ready to hit back.

U.S. businesses lost an average of $289,000 in 2008 to security breaches.† No business or organization can afford exposure to that kind of risk. Educating yourself on the strategies and solutions you need to stop this exposure is your imperative. RSA® Conference is the one place where you can meet with experts, colleagues and vendors to find solutions that will positively impact your information security programs now and in the future. It's a security investment you can count on to deliver results — and it's all at RSA® Conference 2009.



REGISTER NOW

APRIL 20–24, 2009 | MOSCONE CENTER | SAN FRANCISCO

WWW.RSACONFERENCE.COM/2009/US/HNS

ENTER PRIORITY CODE: HN029

†Computer Security International (CSI) Computer Crime and Security Survey, 2008.

TABLE OF CONTENTS

What you have in front of you is the 20th edition of (IN)SECURE. It seems just like yesterday that we announced the magazine at the Infosecurity show in London back in 2005. Much has changed since then: the quality and size of the publication has gone up, a variety of security professionals have chosen us as their voice for the community, and the subscribers list is growing exponentially. Thank you for your support! Do get in touch if you'd like to have your article published or your product reviewed.

Before we put out the next issue of (IN)SECURE we'll be attending InfosecWorld in Orlando (USA), the RSA Conference in San Francisco (USA) as well as Infosecurity Europe in London (UK). If you'd like to meet, drop us a note!

Mirko Zorz
Chief Editor

Visit the magazine website at www.insecuremag.com

(IN)SECURE Magazine contacts
Feedback and contributions: Mirko Zorz, Chief Editor - editor@insecuremag.com
Marketing: Berislav Kucan, Director of Marketing - marketing@insecuremag.com

Prototype of Kaspersky antivirus solution for Windows 7

Kaspersky Lab released a technical prototype of Kaspersky Anti-Virus for Windows 7. The prototype is based on the new antivirus engine which provides complex antivirus protection from all types of Internet threats. The new technical prototype of Kaspersky Anti-Virus is designed to secure computers running under Windows 7. Kaspersky Lab simultaneously released its technical prototype providing greater efficiency and complex antivirus protection for the new operating system. (www.kaspersky.com)

Netgear unveils ProSecure STM series of threat management appliances

Netgear launched its new line of Security Threat Management (STM) products. The ProSecure STM Series offers three platforms, each with a different level of horsepower, to accommodate businesses with up to 600 concurrent users. The STM150, STM300 and STM600 all contain the same security functionality with increasing amounts of bandwidth to support various-sized SMBs.

The ProSecure STM Series sets a new bar for SMB security management. The STM deploys inline in a matter of minutes, anywhere behind the network firewall. It runs automatically and unobtrusively. There is no need to reconfigure mail servers or web proxies, unlike traditional proxy-based security solutions. Administration is performed through an intuitive web-based interface. (www.netgear.com)

Backup and disaster recovery solution for virtual environments

Arkeia Software released Arkeia Network Backup 8 which delivers the first true virtual appliance for backup that gives customers free choice of hardware. The Arkeia Virtual Appliance delivers Arkeia Network Backup as a system image for a VMware virtual machine and comes bundled with everything required to implement a backup solution, including licenses for a disk-based virtual tape library (VTL) and Arkeia Backup Agents. (www.arkeia.com)

Damn Vulnerable Linux 1.5 is now available

Damn Vulnerable Linux (DVL) is meant to be used by both novice and professional security personnel and is even ideal for the Linux uninitiated. You can start learning IT security knowledge domains such as web vulnerability, network security, or binary vulnerability such as exploitation or shellcodes. (www.damnvulnerablelinux.org)

New McAfee SaaS security business unit

McAfee has created a new business unit to enhance and expand the company's software as a service offerings. The business unit will be responsible for all products within McAfee delivered over the Internet, including security scanning services, Web and e-mail security services and remote managed host-based security software and hardware.

McAfee has named Marc Olesen senior VP and general manager of the SaaS Security Business Unit. Olesen was previously VP of SaaS business at HP and has held executive positions at Qwest Cyber Solutions and BearingPoint. He will report to DeWalt and Christopher Bolin, McAfee chief technology officer and executive vice president. (www.mcafee.com)

Free fuzzing utility for Oracle database applications

Sentrigo announced FuzzOr, an open source fuzzing tool for Oracle databases designed to identify vulnerabilities found in software applications written in PL/SQL code. The new utility allows PL/SQL programmers, database administrators (DBAs) and security professionals to identify and repair vulnerabilities that may be exploited via SQL injection and buffer overflow attacks—the most common techniques used by malicious hackers to launch attacks on databases.

FuzzOr runs on Oracle database versions 8i and above to identify coding errors. A dynamic scanning tool, FuzzOr enables DBAs and security pros to test PL/SQL code inside Oracle-stored program units. Once vulnerabilities are detected by FuzzOr, a programmer can then repair the PL/SQL code. (www.sentrigo.com)

First solution for auto-configuration of iPhone VPN access

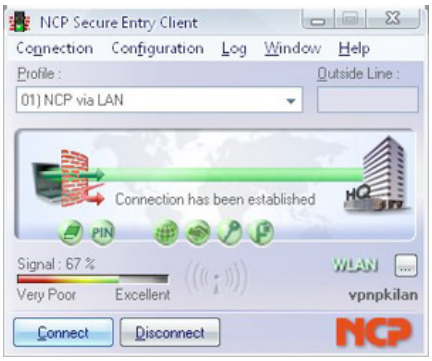
Astaro users with iPhones can now automatically setup a secure, IPsec VPN tunnel with no technical knowledge required.

This new process adds yet another method that iPhone users can use to connect to Astaro Gateway products. In addition to the iPhone's PPTP and L2TP VPN connectivity options, Astaro users can now use the iPhones IPsec VPN capabilities to connect to their home and business networks. (www.astaro.com)

New version of Check Point's secure wireless router Z100G

Check Point released version 8.0 of the Check Point ZoneAlarm Secure Wireless Router Z100G. The new version includes new security features and enhancements, providing advanced enterprise level protection for consumers' home or home office wireless networks. As the first true Unified Threat Management appliance specifically created for consumers, the ZoneAlarm Secure Wireless Router Z100G enables users to surf the Internet with super-fast wired and wireless networking and enjoy the highest level of protection against hackers, malware, identity theft, and more. The Z100G complements the security offered by ZoneAlarm PC software and leverages Check Point's enterprise-class embedded NGX security technologies. (www.checkpoint.com)

First Windows 7 universal IPSec VPN client



NCP engineering has developed the first universal IPSec VPN client for Windows 7. Now available, the beta version of the NCP Secure Entry Client will provide users and IT administrators with a flexible, intuitive solution for secure remote network access.

The client makes VPN security a 'one-click and forget it' experience. Once the client has been installed on a device, beta users can connect to third-party IPSec gateways without needing to change settings or certificates. (www.ncp-e.com)

UPEK launches biometric fingerprint solutions for netbooks

UPEK announced fingerprint authentication solutions for manufacturers of netbooks and Mobile Internet Devices (MIDs) to integrate into these new classes of portable, internet-connected computing devices. UPEK's Fingerprint Authentication Solutions for netbooks and MIDs feature the TouchStrip TCS5 Fingerprint Sensor optimized for compact, low-cost, low-power devices, and Fingerprint Suite Starter software that allows users to access password protected websites with the simple swipe of a finger. (www.upek.com)

Improving network discovery mechanisms

by Fyodor Yarochkin and Ofir Arkin

Remote operating system fingerprinting is the process of actively determining a target network system's underlying operating system type and characteristics by probing the target system network stack with specifically crafted packets and analyzing received response.

Identifying the underlying operating system of a network host is an important characteristic that can be used to complement network inventory processes, intrusion detection system discovery mechanisms, security network scanners, vulnerability analysis systems and other security tools that need to evaluate vulnerabilities on remote network systems.

Remote system fingerprinting is not only an offensive tactics. This technique can also be used as part of a defense strategy. For example, the effective techniques of analyzing intrusion alerts from Intrusion Detection Systems (IDS) consist of reconstructing the attacks based on attack prerequisites. The success rate of exploiting many security vulnerabilities depends heavily on the type and version of the underlying software running on the attacked system and is one of the basic required components of the attack prerequisite. When such information is not directly available, the IDS correlation engine, in order to verify whether the attack was successful, needs to make "educated guess" on possible type and version of software used on the attacked systems. For example, if an IDS captured a network payload and matched it to the exploit of a Windows system vulnerability, the risk of such a detected attack would be high only if the target system exists and is indeed running the Windows operating system and exposes the vulnerable service.

In this article, we'd like to introduce a new version of the Xprobe2 tool (xprobe.sourceforge.net) that is designed to collect such information from remote network systems without having any privileged access to them. The original Xprobe2 tool was developed based on research by Ofir Arkin on remote system discovery using ICMP, and included some advanced features such as use of normalized network packets for system fingerprinting, a "fuzzy" signature matching engine, modular architecture with fingerprinting plugins and so on.

The basic functionality principles of Xprobe2 are similar to the earlier version of the tool: it still utilizes similar remote system software fingerprinting techniques. However, the key focus point of this version is to use minimal number of packets to perform remote network probing. Therefore a few significant changes were introduced to the signature engine and the fuzzy signature matching process.

The key difference in the fuzzy signature matching process is the introduction of the "module weighting" concept (originally proposed by Lloyd G. Greenwald in his academic paper and extended in the current Xprobe implementation). This will be introduced later, in another section of this article.

The tool now also includes components for performing target system probing at the application level. This makes it capable of successfully identifying the target system even when protocol scrubbers (such as PF on OpenBSD system) are in front of the probed system and normalize low-level protocol packet variations.

The use of honeynet software (such as honeyd) is also known to confuse remote network fingerprinting attempts. These honeynet systems are typically configured to mimic actual network systems and respond to fingerprinting attempts. Xprobe2 includes the analytical module that attempts to detect and identify possible honeynet systems among the scanned hosts, or the systems with modified network stack settings, by creating "randomized" application level requests and comparing the results with the results provided by network level probing.

Another key concept introduced with Xprobe2 as an experimental component, is the use of peer-to-peer network architecture between Xprobe2 nodes that allows Xprobe2 instances to share network scanning data between peers and improve performance of large-volume scans.

Active operating system fingerprinting is the process of actively identifying the characteristics of the software which runs on the scanned computer system, using information leaked by the target system network stack.

Remote active network fingerprinting: process and problems

Active operating system fingerprinting is the process of actively identifying characteristics of the software (such as OS type, version, patch-level, installed software, and possibly - more detailed information) which runs on scanned computer system, using information leaked by the target system network stack.

The possibility of performing active "fingerprinting" of network protocol stack exists because the actual protocol implementation within each operating system or software component may differ in details. That is because every operating system network stack is build in accordance to the protocol specification requirements (such as RFC). However, every protocol may have some "gray" areas - states of the protocol, which are not covered, or not covered to the full extent by the protocol specification.

Additionally, there is a number of other critical factors that affect the efficiency and accuracy of the remote network mapping and active operating system fingerprinting scan. Some of these issues are relevant to the way the network mapping tools are designed, while other issues are more specific to the network topology of the scanning environment, underlying data-link type, type of network connectivity to the target and so on.

Depending on the variation of the network configuration, the type of information that we would be able to collect regarding target system would also variate.

In the remaining part of this section we are going to discuss typical problems and issues that a network mapping and active operating system fingerprinting has to deal with while performing the scanning process.

Problem 1: Handling packet filtering nodes and network protocol scrubbers

When packets travel across the network, there is a possibility that these packets (especially the malformed form of the packets, which are frequently used in OS fingerprinting signatures) will be modified, which affects the accuracy of the OS fingerprinting itself. Xprobe2 is aware of this fact and the fuzzy signature matching mechanism is designed to deal with this type of problems.

Furthermore, the use of "module weights" and performing of remote system probing at different layers may compensate incorrect, or false results obtained by particular tests. Moreover, such behavior of some routing and packet filtering devices could be analyzed and signatures could be constructed to identify and fingerprint intermediate nodes.

Problem 2: Detecting modified or altered TCP/IP stacks

Some TCP/IP network stacks may be modified deliberately to confuse remote OS Fingerprinting attempts.

The modern OS fingerprinting tool has to be capable of dealing with this type of systems and of identifying eventual OS stack modification. Xprobe2 does so by using additional application level differentiative tests to map different classes of operating systems.

When application level tests are used along with network level tests, it is much harder to alter system applications to make them behave differently, because such behavior is dictated by the design of the OS underlying system calls. For example, a test that uses 'directory separator' mapping simply tests how target system handles '/' and '\\' type of slashes to differentiate windows hosts from Unix. Additional application level modification would be required (and that is not always easy) in order to trick this test with fake results.

Xprobe2 also includes an application level testing module that randomizes its requests, making it more difficult to implement "fake" responders at application level, unless a real application is running behind.

Problem 3: Detectability of malformed packets

If a remote active operating system fingerprinting tool utilizes malformed packets to produce the fingerprinting results, a filtering device may drop these malformed packets if the filtering device analyzes packets for non-legitimate content. Therefore the quality of the results produced by utilizing a fingerprinting tests relying on malformed packets will be degraded and in some cases even fail.

Malformed packets may produce another effect, they might cause some TCP/IP stacks to crash or lead to excessive alerting by Intrusion Detection Systems. One of the focuses of Xprobe2 is to be able to use "normal" network packets when possible to execute its task. It is possible, by turning certain modules on or off, to perform remote network OS fingerprinting using solely "normal" packets.

(Note: We consider network packets that conform to the protocol specification to be normal).

Xprobe2 architecture overview

The architecture of Xprobe2 includes several key components: the core engine and the set of pluggable modules. The core engine is responsible for basic data management, signature management, modules selection, loading and execution and result analysis. The modules, which are also known as "plugins", provide the tool with packet probes to be sent to the target systems and methods of analyzing and matching the received response to the signature database.

Each of the modules is also responsible for declaring its signature keywords and parsing the data supplied in signature file. In Xprobe2 the modules are also required to provide a method to generate a signature entry for a target operating system. The modules in Xprobe2 are organized in several groups: Network Discovery Modules, Service Mapping Modules, Operating System Fingerprinting Modules and Information Collection Modules. The general execution sequence is shown on the diagram.

Each group of modules is dependent on the successful execution of the other group, therefore groups of modules are executed sequentially. However, each particular module within the group may be executed in parallel with another module within the same group. It is possible to control which modules, and in what sequence are to be executed, using command line switches.

Network discovery modules

The discovery modules in Xprobe2 are designed to perform host detection, firewall detection, and provide information for the automatic receive-timeout calculation mechanism.

There is also a network mapping discovery module that can be enabled to probe a number of hops until the target system, and perform packet filtering rules mapping using scanning techniques similar to Firewalk.

The aim of the network discovery modules is to elicit a response from a targeted host, either a SYNIACK or a RST as a response for the TCP ping discovery module and an ICMP port unreachable as a response for the UDP ping discovery module. The round trip time calculated for a successful run of a discovery module is used with the automatic receive-timeout calculation mechanism. The automatic 'receive-timeout' calculation mechanism is used at a later stage of the scanning to estimate actual target system response time and identify silently dropped packets without having to wait longer.

Xprobe2 introduced a new network discovery module that uses SCTP.

Operating system fingerprinting modules

The operating system fingerprinting modules are a set of tests (with possible results, stored in Signature files), whose primary purpose is to determine the target operating system and architecture details based on received responses. The execution sequence and the number of executed operating system fingerprinting modules can be controlled manually or be calculated automatically using the information discovered by network discovery modules.

Optional port scanning

The key difference of Xprobe2 is that it does not automatically perform port scanning of the targeted system, trying to maintain the minimal usage of network packets for the network discovery. However, the success of some Xprobe2 fingerprinting tests relies on knowing the open TCP port number, or the open/closed UDP port number. Such knowledge can be provided to Xprobe2 via command line tools or the port scanning module that can perform "probes" of the given port ranges.

The key difference of Xprobe2 is that it does not automatically perform port scanning of the target system, trying to maintain the minimal usage of network packets for the network discovery.

Module execution and signature matching

Xprobe2 stores OS stack fingerprints in form of signatures for each operating system. Each signature will contain data regarding issued tests and possible responses that may identify the underlying software of the target system.

Xprobe2 was the first breed of remote OS fingerprinting tools that utilizes a "fuzzy" matching algorithm during the remote OS fingerprinting process, and we believe Xprobe2 is the first tool that utilizes controlled reordering and execution sequence of remote module fingerprinting tests based on the concept of module weighting (discussed later in this section).

The primary achievement of this tactic is the minimization of network packets used in remote fingerprinting, a lower detectability rate and improved accuracy of fingerprinting results; which might be affected by failed tests, responses to which were altered by TCP/IP stack modification suites.

With "fuzzy" signature matching, Xprobe2 is able to handle the situations when no full signature match is found in the target system responses - Xprobe2 provides a best effort match between the results received from fingerprinting probes against a targeted system to a signature database.

Xprobe2 currently uses one of the simplest forms of fuzzy matching, which is similar to those used in Optical Character Recognition (OCR) algorithms, by utilizing a matrix-based fingerprints matching based on the statistical calculation of scores for each test performed.

Xprobe2 signatures are presented in human-readable format and are easily extendible. Moreover, signatures for different hosts may have different number of signature items presented within the signature file. This allows the tool to maintain as much as possible information regarding different target platforms without need to re-test the whole signature set, when the system is extended with new fingerprinting modules.

The "fuzzy" matching of signatures is based on a simple matrix representation of the scan (or scans), and the calculation of 'matches' is performed by simply summing up scores for each 'signature' (operating system). All tests are performed independently.

As the tool progresses with the target system probing, the matrix is being filled with score values that signify how well the received response matches the signature of each operating system and reflects the module weight in the final decision-making process.

When the scan is completed, the total score is calculated and the highest-matching signature (or a list of possibly matching signatures) is given as the final result.

Xprobe2 signatures are presented in human-readable format and are easily extendible.

Module weighing

The module weighing mechanism is based on the publication by Lloyd G. Greenwald from LGS Bell Labs on Evaluation of the operating system fingerprinting tests.

The primary consideration is as following: each network probe (packet) that is sent over a network incurs a cost (time for sending the packet and waiting for response, used network traffic and so on). If the network probe uses a malformed network packet, the cost is doubled, as this increases the possibility of being detected or even crashing the remote system.

Furthermore, each network test generates a different "amount" of information (so called information gain) and has a different impact on the entropy measure of the final result: guess of the target operating system.

The information gain for each test can be calculated by analyzing the total number of possible final results, which would be caused if the test probe responds with a certain value. Furthermore, each of the tests might be characterized with reliability (which is 1 by default, but can be changed through the signature file), which affects the modules' information gain.

The primary motivation in selecting the module execution sequence is to re-order tests based on their costs (lower cost leads to lower detectability of the scan, lower bandwidth usage and so on), higher-information gain (which leads to a higher accuracy of the test), or the optimal balance between the cost and obtained information gain.

The test motivation in Xprobe2 can be controlled with command line switches.

Experimental P2P architecture

The P2P framework prototype will be released as an additional component to Xprobe2 and is (at the current stage) a totally experimental approach to improve large-scale network scanning/fingerprinting processes by providing a medium for scanning nodes to pre-share scanning information.

The basic idea is to institute a cooperative peer-to-peer information sharing network where each of the peers can, prior to scanning, perform queries on data availability within the network and then can scan (and contribute) only the data which is not currently found within the network.

The contributed data is randomly verified by other peers and cryptographically signed to ensure that no bogus data is submitted.
The search queries may include IP ranges, type of scans, and time characteristics, which would also allow the network users to perform so called 'delta' scans - scans that aim at detecting changes within the probed network environment.

This is still an ongoing research project and more documentation will be released when the project reaches a certain stage of maturity.

Conclusions

Our tool provides high performance, high accuracy network scanning and network discovery techniques that allow users to collect additional information regarding scanned environment. Xprobe2 is focused on using minimal amount of packets in order to perform active operating system fingerprinting, and that makes the tool suitable for large-scale network discovery scans.

Xprobe2 is also focused on using tests that utilize normal, non-malformed packets (this behavior can be controlled with command-line switching), which should guarantee that no network system or network device would crash as a result of Xprobe2 probing.

It is still possible to evade fingerprinting and confuse application-level fingerprinting modules, however no existing software has out-of-box features designed for this purpose, which makes such evasion a relatively complex task.

NOTE: The new version of Xprobe2 and the complementary technical paper will be released in June 2009.

Reference

Author: Lloyd G. Greenwald and Tavaris J. Thomas
Title: Towards Undetected Operating System Fingerprinting
Published: WOOT'07: Proceedings of the first USENIX workshop on Offensive Technologies
Year: 2007

Yarochkin Fyodor is a graduate student at the National Taiwan University and a member of o0o Security Research Group (www.o0o.nu), focusing in his reseach on offensive technologies, distributed dependable systems and network security. Fyodor is also known for his contributions to the Snort Project.

Ofir Arkin is the co-founder and CTO of Insightix and Sys-Security Group (www.sys-security.com), known for his research on ICMP usage in network scanning and VoIP security. He is also an active member of the Honeynet project and has participated in writing the Honeynet team book "Know Your Enemy", published by Addison-Wesley.

Building a bootable BackTrack 4 thumb drive with persistent changes and Nessus

by Kevin Riggins

Last year I was in South America and needed to be able to perform some scans and tests on a network. There was one problem though. I was not allowed to connect my laptop to their network. However, I was allowed to use any software I wanted on one of their machines. BackTrack to the rescue.

BackTrack is a Linux distribution focused on penetration testing. The folks at www.remote-exploit.org gathered together a collection of over 300 open-source tools and created a Live CD/DVD that contains them all. You can boot the live CD/DVD in a few minutes and be ready to get to work.

While this is really handy, there is a one problem with the live CD distribution format. You can't save any information to the CDROM. In other words, once you have done some work, you have to figure out how to save that work to another medium.

Never fear! The BackTrack team kept this in mind when they created the distribution. They made it possible to fairly easily configure a USB thumb drive to save or persist changes.

At the time, the version of Backtrack available was version 3 and that was what I used. Since then, Backtrack 4 Beta has been released.

In the Backtrack 3 version of this how-to, which is still available on my website (www.infosecramblings.com), there were a few other issues I wanted to address in addition to making changes persistent. I wanted to add one tool and update two others to versions that were released after the release of BackTrack 3. The tool I wanted to add was Nessus. Nessus is a vulnerability scanning application. It scans for an ever increasing number of known vulnerabilities in systems and devices.

The tools I wanted to update were Firefox and Nmap. We still need to add Nessus, but lucky for us, Backtrack 4 Beta already has the latest versions of Firefox and Nmap.

This article will walks through setting up a bootable BackTrack 4 Beta USB thumb drive with the following features:

- Persistent Changes
- Nessus and NessusClient installed.

Assumptions, tools and supplies

This guide is written with the following assumptions:

• You know how to partition and format disks.
• You are familiar with Backtrack.
• You are familiar with Nessus.
• You are familiar with Linux.
• You are familiar with Windows.

Tools and supplies

• A USB thumb drive - minimum capacity 2GB
• A Backtrack 3 CDROM, Backtrack 4 DVD or an additional USB thumb drive (minimum 1GB in size) - Used to partition the thumb drive.
• UNetbootin (unetbootin.sourceforge.net) - A free tool to transfer an iso image to a USB drive.

Let's get started!

Partitioning the USB thumb drive

If you have a Backtrack 3 CD or Backtrack 4 DVD, you are in good shape. If you don't and are using an additional USB thumb drive, you are going to need to skip ahead to the 'Making a bootable Backtrack 4 thumb drive' first so you have something to use to partition the target drive. Return to here once you have some form of bootable Backtrack. I know this seems convoluted, but it's the easiest and most sure way I know to get us where we want to go.

First let's partition our thumb drive. I used a 4 GB drive as I read that we would need 1.2 GB for persistent changes. After I got everything working, it looks to me like we can get away with a 2 GB stick if we are careful about regular cleanup of log files. Nessus tends to be the main culprit here.

Regardless of the size thumb drive we use, we need to partition and format the drive as follows:

The first partition needs to be a primary partition of at least 1 GB and formated as FAT32. The second Partition can be the rest of the thumb drive. It needs to be formatted as ext2.

If you try to use Windows to re-partition the drive, you will likely run into some problems. Windows sees most USB thumb drives as removable media. As such, it does not support multiple partitions on them. It also does not allow us to delete the existing partition from the drive. This is because most thumb drives have the 'Removable Media Bit' set. One of the reasons for this is so that autorun will work.

The easy way to get around the problem is to re-partition the drive using Linux. That's why we need the Backtrack CDROM, DVD or additional thumb drive although any Linux system will work. So go ahead and partition and format the drive according the layout above. Once I was done with this step, I switched back to a Windows system for the next few steps.

Make a bootable Backtrack 4 USB thumb drive

Now we need to download the Backtrack 4 ISO. Here are the details about the distribution package and the location to download it from. As always, check the hash values to make sure you are getting what you expect.

Description: DVD Image
Name: bt4-beta.iso
Size: 854 MB
MD5: 7d1eb7f4748759e9735fee1b8a17c1d8
Download:
www.remote-exploit.org/cgi-bin/fileget?version=bt4-beta-iso

In the last step we partitioned our USB thumb drive to have at least one 1 GB FAT32 partition on it.

The next step is to make it a bootable USB thumb drive. This used to be fairly complicated, but now there is a much easier way. We are going to use the UNetbootin tool mentioned above. It is super easy to use. Just start UNetbootin, select the Backtrack 4 ISO, select the USB drive and click okay. You may get a warning that files exist on your USB drive.

After making sure you picked the right one, tell it to go ahead and replace the files. It'll chug along and before you know it you will have a bootable thumb drive. Much easier than the rigmarole we had to go through before.

In some cases, the thumb drive will may not be bootable after running UNetbootin. If this happens, from Windows, open a command window and do the following.

Change to the drive letter that your thumb drive is mounted on.

```
cd /boot
execute bootinst.bat
```

Note: we need administrative privileges for this.

Enabling persistent changes

Once we have booted into Backtrack we need to configure the rest of the thumb drive if we haven't already done so. I used fdisk to create a second partition from the remainder of the drive and formatted it with `mkfs.ext2`. In my case my USB drive was `/dev/sdb`.

Once we have formatted a second partition, mount it and create a changes directory in the root of the file system. Open a terminal windows and execute the following commands:

```
mount /dev/sdb2 /mnt/sdb2
cd /mnt/sdb2
mkdir changes
```

Next we need to make some changes to how the system boots. Execute the following:

```
cd /boot/syslinux
chmod +Xx lilo
chmod +Xx syslinux
```

Open `syslinux.cfg` with your favorite editor and make the following change. Note: I copied the boot definition I wanted to change and created a new entry so I would have a fall back option if broke something beyond repair.

Find the line "LABEL BT4".
Copy that line and the next three right after that section.
Change the "LABEL BT4" to something you want like "LABEL BT4-persist" and description to something like "MENU LABEL BT4 Beta - Console - Persistent"
Change the line that begins with APPEND in your copied section by adding `changes=/dev/sdx2` immediately after `root=/dev/ram0 rw` where the x is the drive appropriate for your system. In my case it looks like this,
`...root=/dev/ram0 rw changes=/dev/sdb2...`
Save your changes and exit the editor.

That should do it. Reboot and select the option you configured. To test it, create a file and reboot again. If your file is still there, everything is golden.

Installing Nessus

Now that our changes are saved from boot to boot, we can install things and they won't disappear on us :)

First we need to get a copy of Nessus. Go to nessus.org and download the Ubuntu Nessus and NessusClient packages. I used the 32-bit 8.04 version which worked fine for me.

We had to jump through quite a few hoops to get Nessus running on Backtrack 3. Again, with Backtrack 4 things are little easier. To install the Nessus server, open a terminal window and simply execute the following command. This assumes you are in the same directory as the Nessus packages.

```
dpkg --install
Nessus-3.2.1-ubuntu804_i386.deb
```

Things are little bit more complicated for the client. There are some dependencies that need to be installed first. Luckily, we have apt to help us with this. Execute the following command to install them. It is all one line.

```
apt-get install libqt4-core libqt4-
gui libqtcore4 libqt4-network libqt4-
script libqt4-xml libqt4-dbus libqt4-
test libqtgui4 libqt4-svg libqt4-
opengl libqt4-designer libqt4-
assistant
```

After that, we can install the client package.

```
dpkg --install
NessusClient-3.2.1.1-ubuntu804.i386.d
eb
```

Finally it's time to configure Nessus. Execute each of the following and follow the prompts provided.

```
/opt/nessus/sbin/nessus-mkcert
/opt/nessus/sbin/nessus-adduser
```

Nessus requires that you have a key in order to keep you plugins up-to-date. You can go to the following link (tinyurl.com/cfb6u) to register for a free home feed. Remember to use appropriately according to the licensing agreement.

Once you have your key, execute the following to update your plugins.

```
cd /opt/nessus/etc/nessus
/opt/nessus/bin/nessus-fetch --regis-
ter [you feed code here]
```

When that is done, and it is going to take a few minutes, you are ready to start the server and client.

```
/etc/init.d/nessusd start
/opt/nessus/bin/NessusClient
```

There you have it, a bootable USB thumb drive with Backtrack 4, persistent changes and Nessus. Now you are fully equipped to go forth and perform penetration tests with the latest tools and without the fear of losing all the work you have done because it didn't get saved.

Kevin Riggins, CISSP, CCNA is a Senior Information Security Analyst for Principal Financial Group. He leads the Security Review and Consulting team which is responsible for performing security risk assessments and providing internal information security consulting services to the enterprise. He also writes on various topics related to information security at www.infosecramblings.com and can be reached at kriggins@infosecramblings.com.

Review: SanDisk Cruzer Enterprise

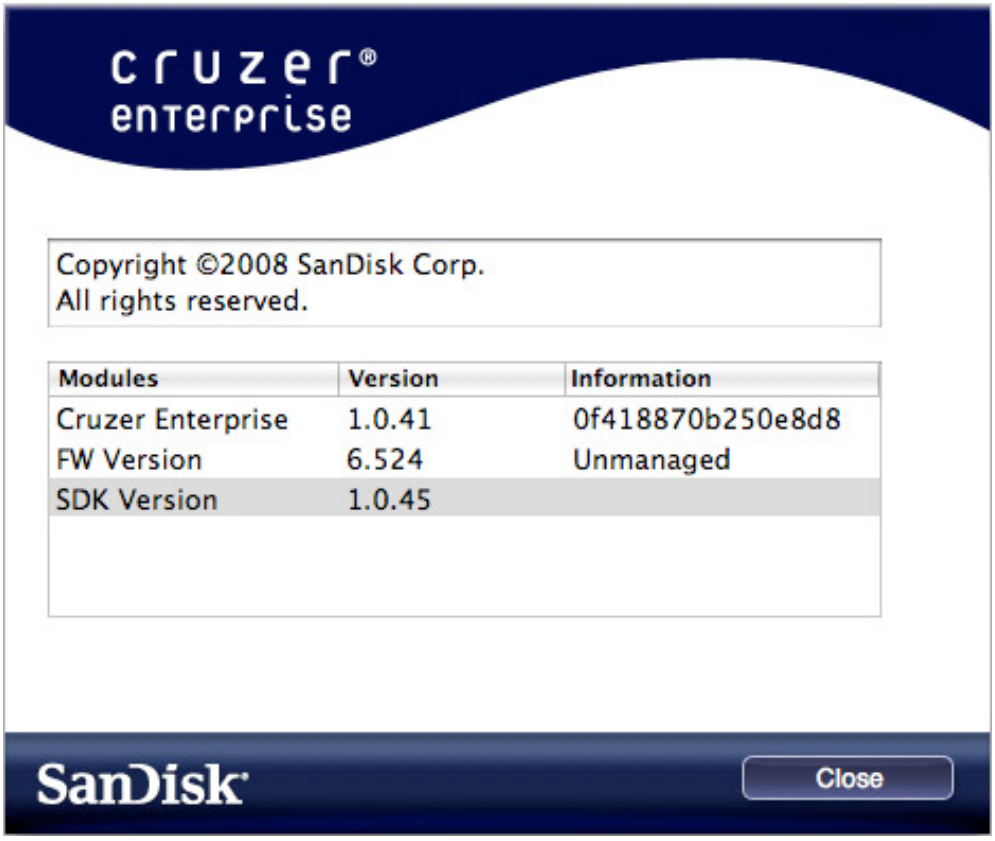
by Mark Woodstone

I planned to start this review by referencing one of the latest news items or surveys on portable storage mishaps. While browsing the Help Net Security (www.net-security.org) archives and doing some additional research via Google, I came across so many horrid stories that clearly indicate a definitive need for using protection for external storage media. Besides losing laptops with loads of private data, which is obviously a trend nowadays, a vast collection of bad scenarios was dealing with USB flash drives. Their biggest practical side - the size - unquestionably generates a lot of problems for regular computer users and even worse, enterprises. With flash drives becoming keychain accessories, they are becoming more and more of a hassle if you have security and privacy in your mind.

One of the best solutions for keeping the data on a flash drive secure is to enforce encryption. Combining regular flash drives with third party crypto applications is not the best way to go - you would still depend on the user to make an extra effort. I recently got a hold of USB flash drive that is a ideal solution for this kind of a scenario - the SanDisk Cruzer Enterprise.

SanDisk is one of the largest, if not *the* largest supplier of flash data storage cards. I have been using their cards in various digital cameras for ages and I was always satisfied with the speed and resilience they provided. In early December 2008, SanDisk announced that SanDisk Cruzer Enterprise became the first secure USB flash drive that fully supports Apple Mac OS X computers. As I am using a Mac outside of my work environment, I was ecstatic with Mac support for this kind of a device. The charts showing Apple hardware sales has been going up for years and providing enterprises with a solution that works on both regular PCs and Macs is certainly a good path for SanDisk.

The article will focus on the device usage related to Mac OS X 10.5.6, on my 2.4 GHz Intel Core 2 Duo iMac boasting 4 gigs of RAM. The computer provides good performances and while I am not the type of guy who is into benchmarking, I will share some data on the speeds I got. Read on for the details. From what I understand, the software application and usage on Windows PCs is absolutely the same, so there is no need to skip this article just because you don't use Mac OS X as your choice of operating system. The device is beautiful because it provides cross platform opportunities for people like me that need to work with both Apple's and Microsoft's operating systems.



Details on the device version and modules

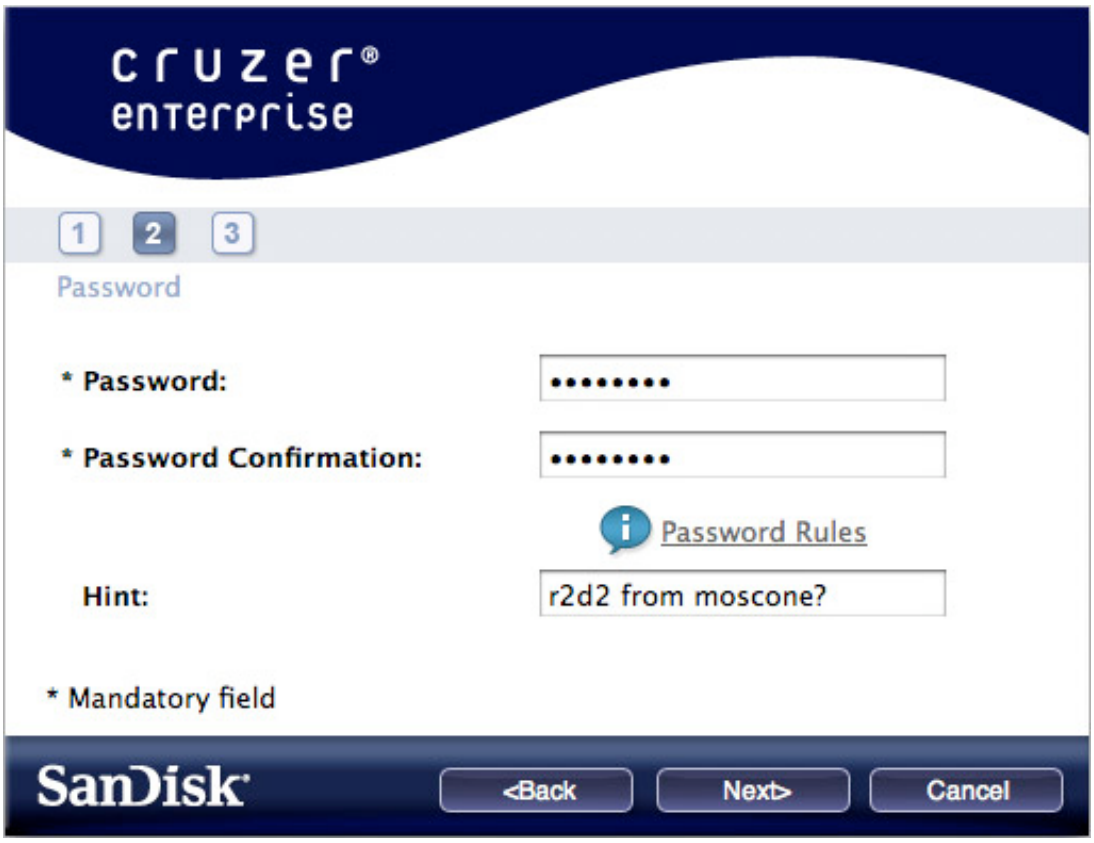
Look and feel

The device I got from SanDisk is a SanDisk Cruzer Enterprise with 2 GB of storage. It is also available in different sizes - a smaller 1 gig one, as well as 4 and 8 GB configurations.

The USB flash disk chassis is smooth and features a pocket clip, as well as an option for using it with a necklace strap. From the eye candy point of view, front side boasts a small imprint that identifies the device as a 2GB model. Just below that, you will find an indicator that flashes in blue color when the device is being used. Removing the cap from the device shows the USB connector. From the size perspective, SanDisk Cruzer Enterprise is as small as your average USB flash drive.

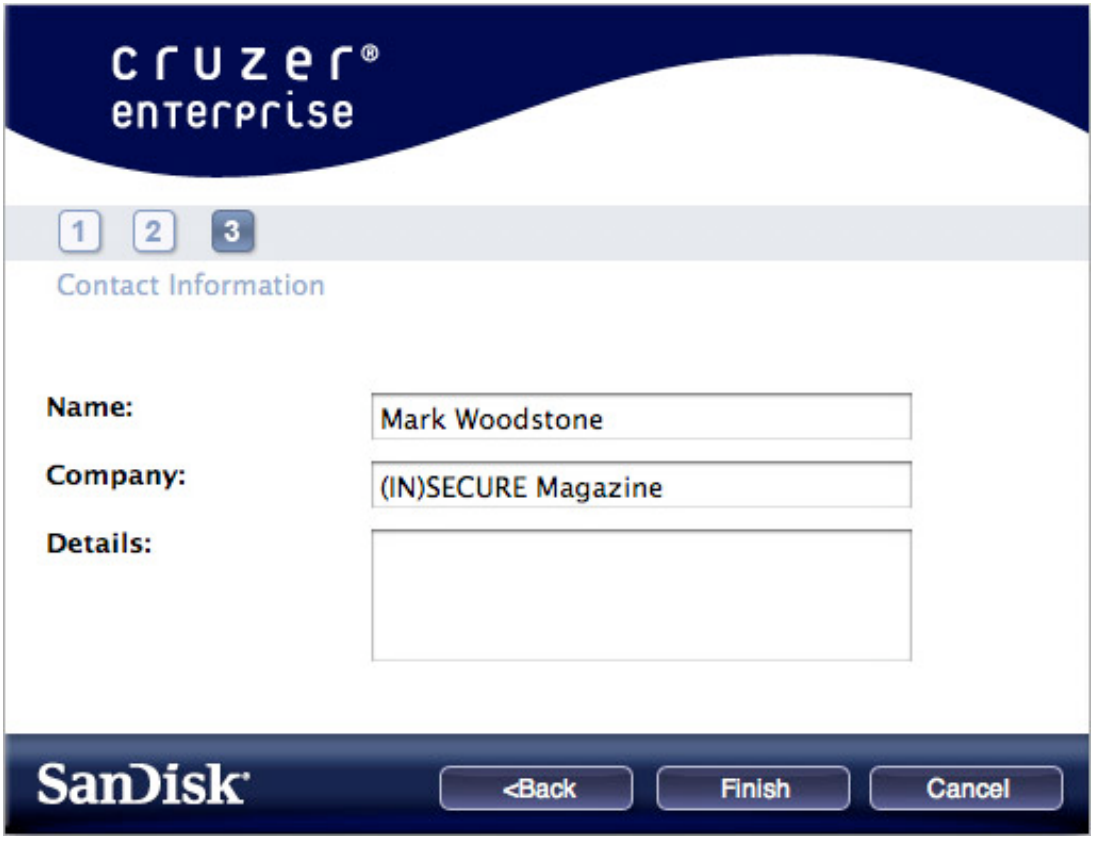
Installation

As soon as you plugin the device into your USB port, a finder window automatically opens and provides you with a .pkg based installer. The installation process is rather typical, you need to agree to the terms of use, input your basic information and setup your initial password. The installer encompasses a set of password rules - no short passwords, you need to have at least one uppercase character and use either one of the numbers or special characters. You would think that this kind of simple, but effective security starting point is somewhat of a standard within security applications - trust me, that's not the case. Good work SanDisk for making a standalone Cruzer Enterprise user unable not to deploy his or her cat's name as a password.



Setting up the password and accompanying hint

While I usually don't use password hints, in some cases they prove to be a lifesaver, so as you can see, I entered one of the most obscure password references ever. Clicking the finishing button sets up the user credentials, initializes the application and a restart of the computer is needed to make everything fully functional.



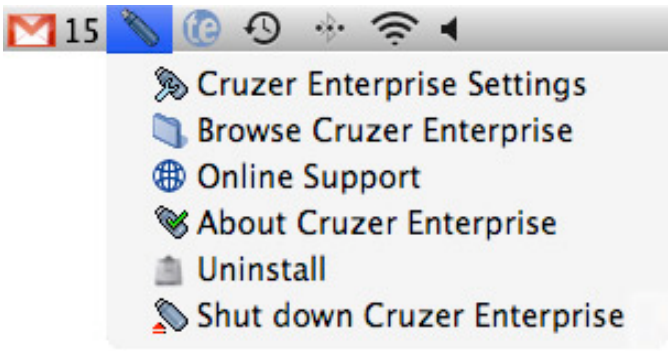
Device owner details

Usage

When the system restarts, Sandisk lipstick-like icon will appear in your applications bar and you will get a window asking for your password. As soon as you type it in, a volume called Enterprise will automatically show in your Finder.

There are some ways to improve this login process. First, it would be nice to have some kind of a check mechanism that doesn't open the "enter password" interface together with the previously mentioned "SanDisk installer window".

This happens every time you restart the computer and of course have the device plugged in the USB port. Luckily, the window gets automatically closed after 3-4 seconds, but we could definitely do without it - the software is already installed, there is no need for the repetitive auto-starting the installer.



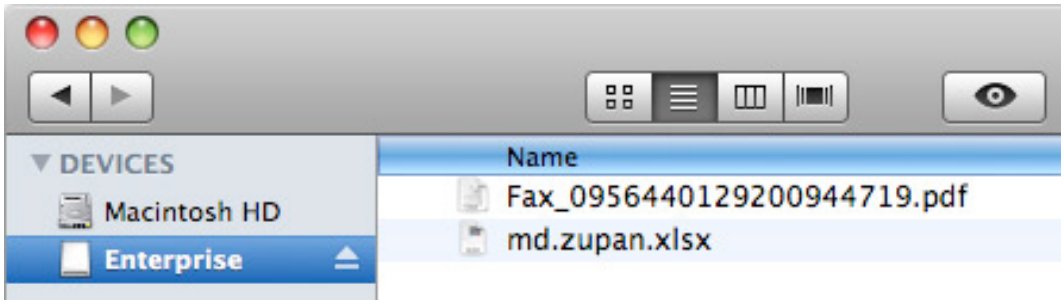
Cruzer Enterprise application options

The second small issue I noticed is that when you enter the password, the application probably works on starting the encrypted volume but the user is greeted with the "spinning wheel" that is associated with unresponsive programs. I can't count the number of times I have seen the spinnig wheel when my Safari goes berserk, so I don't like seeing this icon when the Cruzer Enterprise app is processing data.

The good news is, these two small things - I wouldn't even call them issues - are the only negative aspects of the device.

From the user perspective there are no specific details to discuss about the usage of this secure drive.

After the successful authentication it works as a typical flash storage disk. Under the hood you have a hardware based 256-bit AES encryption with mandatory access control for all files on 100% private partition. There is a lockdown mode that is obviously used for locking down the device in a case someone tries to get unauthorized access to your stored files.



Sample files stored in the Enterprise volume

Previously, when I talked about the password policy, I mentioned a device usage in a standalone mode. I just need to follow up on what I had in mind.

As SanDisk Cruzer boasts with Enterprise in the product's name, you probably understood that there is some "higher software power" that can work its wonders with this nifty device. CMC, or Centrally Managed Control is SanDisk's enterprise data management software that can be used for managing company-issued Cruzer drives.

The software solution is of course sold separately, but provides enterprises with some fantastic opportunities such as integration with Active Directory (for device-user associations and password policies), centralized application distribution (probably both internal apps, as well as partner software such as McAfee option that provides an extra layer of protection with malware scanning), auditing functionality for regulatory compliance, as well as RSA SecureID authentication integration. These are just some of the more powerful options of managing Cruzer drives through CMC.

Speed

The product support page boasts with the following figures based on their internal testing: 24MB/s read and 20 MB/s write. I have tested read/write speeds on my computers and here are the details.

Write scenario - the computer doesn't have any open application other than the system ones, SanDisk app and Google Notifier. I transferred a 1.71 GB folder from my Desktop to the Enterprise volume. It took 97 seconds, which ends up about 18.05 MB/s write option.

Read scenario - the computer has a couple of applications open, my backup is being actively downloaded from a remote server. I transferred a similar 1.71 GB folder from the Cruzer drive to my documents folder. It took 69 seconds, which ends up about 25.37 MB/s which is even better then what the specs say.

Final thoughts

Overall, I am quite satisfied that I finally have a secure USB storage drive that can work on both my home Mac, as well as my company PC workstation. The SanDisk Cruzer Enterprise installation and usage is piece of cake and I am really happy for the latest addition to my tech arsenal.

Mark Woodstone is a security consultant that works for a large Internet Presence Provider (IPP) that serves about 4000 clients from 30 countries worldwide.

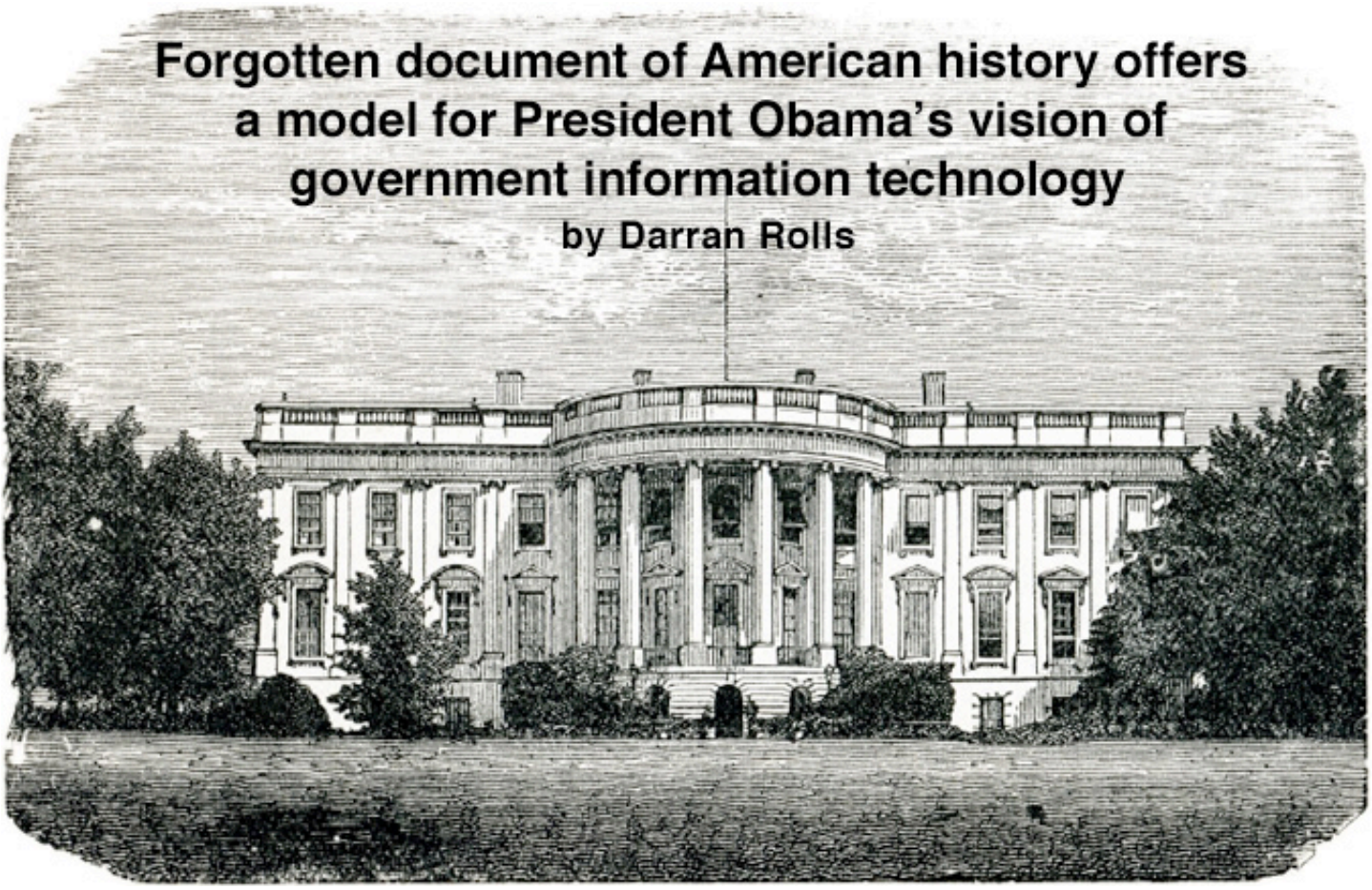
HELP NET SECURITY

WWW.NET-SECURITY.ORG

10 years of information security coverage

Forgotten document of American history offers a model for President Obama's vision of government information technology

by Darran Rolls



From 1781 to 1787, the newly independent United States of America tried to govern itself as a loose federation of states bound by the Articles of Confederation. By 1787, however, the states realized they needed a stronger central government, adopted the Constitution, and consigned the Articles of Confederation to the historical backlot. 222 years later, as President Barack Obama takes the reins of government with the promise of revamping its use of technology, the federation concept could be making a comeback in the form of an information technology model that supports the new president's ambitious technology agenda.

Obama's vision for government information technology, if realized, will completely change the way information flows through and between public agencies and private citizens. His goals touch everything from expanded broadband to tech training for workers, but one of them in particular portends massive change for government IT staffs: creating a transparent and connected democracy. On the Obama-Biden Web site, there are two sub-points supporting that goal.

The first is opening up government to its citizens by using "cutting-edge technologies to create a new level of transparency, accountability and participation for America's citizens." The second is bringing government into the 21st century by using technology "to reform government and improve the exchange of information between the federal government and citizens while ensuring the security of our networks."

The government needs a completely new IT model to support Obama's goals. As they're currently conceived, government IT systems can't be as open as he wants them to be without inflating IT overhead costs. Today's government IT faces inward. Its role is to manage information for internal use. When a citizen wants that information, they file a request and a government employee retrieves it. Although government has been computerized for decades, most agencies have only computerized the process of requesting information.

They have not provided direct access to the information itself. In this regard, IT systems are just digital extensions of paper records.

Obama has called for appointing a national chief technology officer to oversee efforts to create a more transparent, interactive government through technology. This person has a daunting job in front of them on an unprecedented scale. Essentially, the national CTO is looking at the biggest ever IT merger & acquisition exercise. Making government IT systems work together across departmental lines is comparable to acquiring a new company and rolling together the data centers and front offices. Departments will have to assess their current staffs and their duties, and transition them to new roles as required. IT systems need the same scrutiny. On the security front, departmental IT staff will have to conduct audits and analyses to identify risks and compliance obligations. The U.S. government is bigger than the Fortune 50 combined. The government has a "customer base" of 220 million people and employs almost 2 million non-military and postal workers in thousands of public agencies.

There are very few IT infrastructures that support such huge numbers, which leaves the national CTO practically no existing model to follow. Nevertheless, there are architectural models in private industry that can help guide the federal government's efforts to balance openness and security on the way to a more responsive IT infrastructure. One in particular, the federated model, has both the scalability and flexibility that such a huge job demands. Already proven in corporate environments, federated computing would enable the government to serve a huge new user base and minimize risk to vital information without inflating management expenses. Although it would have to be adapted to work on the federal government's scale, its principles are sound for a project of this size.

Stress is on service

If you strip away the rhetorical flourishes, Obama is saying that he wants government IT to provide the same level of personalized service as the best private corporations. Faster, easier access to information will give government the transparency Obama envisions. He uses the term "openness" interchangeably with transparency, but openness *per se* isn't the government's problem. The U.S. government is already extraordinarily open in most respects. Government agencies constantly push information toward the public, and the Freedom of Information Act ensures access to most government documents.

The problem is that it's not always easy to find what you're looking for, and even when you do, you're often dependent on someone to unlock it for you, or to send a physical document. That abridges the openness by making the process more onerous and therefore more costly than need be. The federal government clearly has a long way to go on that path. Before the federal government charges down that openness path, however, consider Obama's other priority, which is "ensuring the security of our networks." Openness and security are fundamentally antagonistic. In this respect the federal government is not comparable to private industry.

Private companies are at much more liberty to restrict access to their information except where mandated by law to provide public access. That affords would-be identity thieves far fewer avenues for breaking into data systems. In government, the presumption is that information should be open to all.

Government agencies, which collect far more information on individuals then private companies, put much more at risk when they offer the kind of openness Obama envisions. Whoever Obama appoints as federal CTO has to reconcile the conflict between openness and privacy before his vision can become reality.

Opening the single path to request

He doesn't say it explicitly, but Obama is clearly calling for government IT infrastructures that support the same kind of Web-based self-service and content personalization consumers expect from their bank, health insurer and favorite e-retailer. That means giving consumers the ability to log into IT systems over the Web, search, retrieve, modify and delete information without human intervention. Based on the citizen's identity, systems should push relevant information their way.

Identity systems need to be interconnected, so that logging into on agency's system could also provide access to another (single sign-on), reducing the need for multiple logins and multiple passwords.

To illustrate how systems like this would work in practice, consider a hypothetical example of a man who logs into the Internal Revenue Service Web site. He wants to check on federal tax codes for the limited partnership he is forming to develop a piece of software he wrote in his spare time. After bookmarking the information he needs, he navigates to the U.S. Patent Office Web site to check on the progress of a patent application he filed. The agency has already notified him via automated e-mail that a hearing on the patent has been scheduled, but he wants to re-schedule the hearing. The system accepts the request and confirms it via e-mail. Before logging off, the man scans the personalized navigation bar that appears whenever he logs onto a government site.

Because all of his personal data in government systems is connected together using a controlled "attribute sharing model", the system knows our entrepreneur has registered his interest in FDA alerts around his ongoing hypertension problem (doubtlessly caused by the nature of his profession). He dynamically receives an FDA alert on his navigation bar that indicates a new variant of his blood pressure medication just entered clinical trials. Interested to find out more, he signs up there and then for an e-mail notification when medication clears its trials. This process reminds our entrepreneur to click through his government data profile and update his preferences at the FDA and at the same time to update his shared email address in order to receive this email on his phone/handset.

This is an example of how an integrated identity management infrastructure could enable government agencies. An identity aware infrastructure model, one that fully supports a secure, federated identity model will enable government to balance the desire for openness with the need to protect sensitive data, while keeping overhead expenses under control. The next generation of identity enabled infrastructure will enable users to access information from a wide range of systems, while maintaining the security and integrity of the over-all system. Next generation of e-Government must provide a holistic approach to its identity management infrastructure if it is to provide a comprehensive approach to the services and user experiences that will be built upon it.

Applying identity management to government scale

Over the past 10 years, the commercial sector has undergone a virtual renaissance in how it manages our identities. This process is still underway as companies move from fragmented, isolated user repositories, to a highly interconnected "federated identity" system and a holistic identity governance model. Without getting into the weeds, this simply means that we have learned that identity records sit at the center of a security architecture that promotes the controlled sharing of identity data, while providing a governance and control model for the owner of the identity records. Federated identity technologies will allow each agency to maintain its own identity records, while promoting a controlled flow of information about those identities to be passed between the agencies on a "need to know" basis.

In the federated model, control over the connections between agencies can be passed to the identity itself. That means that you and I get to decide if the FDA should connect with the Labor Department around our identity records. It also affords the agencies themselves a higher level of visibility and control over what information (identity attributes) are being shared. In short, the agencies get all the benefits of a single centralized identity "repository", without the need to go out and actually create one.

The idea of a single central agency that's in charge of an all knowing electronic identity repository makes privacy advocates cringe. A federated identity model could, however, allow each identity a choice when records are shared and when they are not. It could also allow each identity -- each citizen – the ability to view and control what information from their identity records gets shared between those agencies. The measure of personal privacy in a newly connected e-Government world

comes from an individual's visibility and control in information sharing process.

With the identity (or citizen) in control of the identity information flow, the agency is free to concentrate on the security model. Based on each identity, each agency must decide who is entitled to get access to what. Access to information must be subject to control and access control must be an intimate part of a holistic approach to identity management.

With millions of users and millions of individual access entitlements, it's easy to see why we see so many "fine-grained access-control" (often referred to as entitlement management) issues. It's fair to say "Houston, we have a problem" – a significant management problem. The past 10 years of dealing with this problem in the private sector has lead to a growing acceptance of a "role based" approach to managing the association of identities to entitlements. Role-based access control (RBAC) has become the predominant model for managing complex access control on a large scale. By grouping identities into roles and associating entitlements to the roles (rather than the individuals), we are able to scale the access-control process. By bring together RBAC techniques with federated identity models, we can create a scalable identity and access infrastructure able to deal with the challenges of government scale.

An enduring confederation

The Constitution replaced the Articles of Confederation because the states needed a strong central government to keep the peace, settle cross-border disputes, and deal with foreign powers as a unified entity. The Articles of Confederation have little enduring legacy, other than showing the states the folly of trying to exist autonomously in a weak framework and creating the environment that produced the Constitution.

Carrying this conceit over to IT begs the question: why not skip the federation stage and go right to a tightly unified "constitutional" federal IT infrastructure? If a loose confederation of federal IT systems can deliver the openness, responsiveness and security that President Obama envisions, why wouldn't strong central control do the job better?

The answer lies in both the technical and ethical realms. The sheer mass of the federal government would make a centrally controlled corporate IT model horrendously expensive and perhaps even impossible given the current technology. From a management perspective, trying to balance the needs of departments with widely diverse needs and missions would be inefficient and a never-ending source of bureaucratic infighting, at best.

The concept of a single federal entity that controls every aspect of information technology, from collecting data to setting policies to managing identities, also has serious ethical implications for personal privacy.

Creating an agency that has a complete digital portrait of individual citizens, from their Social Security numbers to medical records to military service records to lists of information they've viewed, creates the potential for huge damage and loss of privacy. An uber-IT agency would be an irresistible target for internal and external thieves. Americans, traditionally wary of too much power in one place, are unlikely to approve of such a system, regardless of the transparency and responsiveness it promises.

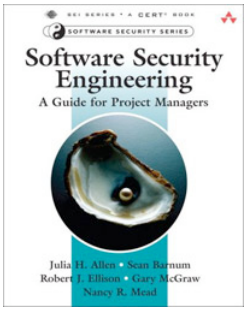
A strong identity management infrastructure based on the federated computing model, however, balances benefits and risks. It keeps policy making, data collection and access management decentralized among the various agencies and departments while providing an enhanced and integrated user experience. Properly implemented, this model is the most promising platform for the government technology infrastructure that President Obama envisions, one that informs the citizenry, gains their trust, and protects their privacy.

Darran Rolls is CTO of Austin, Texas-based SailPoint Technologies (www.sailpoint.com).

Software Security Engineering: A Guide for Project Managers

By Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead

Addison-Wesley Professional, ISBN: 032150917X

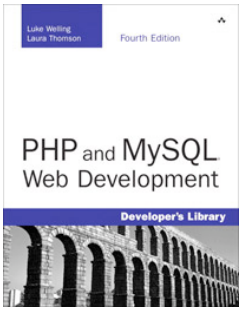


Software Security Engineering draws extensively on the systematic approach developed for the Build Security In Web site. Sponsored by the Department of Homeland Security Software Assurance Program, the BSI site offers a host of tools, guidelines, rules, principles, and other resources to help project managers address security issues in every phase of the software development life cycle. The book's expert authors, themselves frequent contributors to the BSI site, represent two well-known resources in the security world: the CERT Program at the Software Engineering Institute and Cigital, a consulting firm specializing in software security.

PHP and MySQL Web Development (4th Edition)

By Luke Welling and Laura Thomson

Addison-Wesley Professional, ISBN: 0672329166

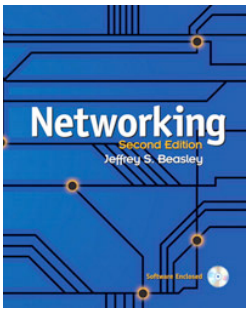


This practical, hands-on book includes numerous examples that demonstrate common tasks such as authenticating users, constructing a shopping cart, generating PDF documents and images dynamically, sending and managing email, facilitating user discussions, connecting to Web services using XML, and developing Web 2.0 applications with Ajax-based interactivity. The fourth edition of the book has been thoroughly updated, revised, and expanded to cover developments in PHP 5 through version 5.3, such as namespaces and closures, as well as features introduced in MySQL 5.1.

Networking (2nd Edition)

By Jeffrey S. Beasley

New Riders Press, ISBN: 0131358383

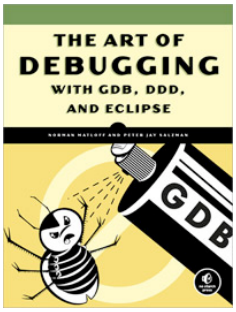


This book provides a comprehensive look at computer networking from the point of view of the network administrator. It guides readers from an entry-level knowledge in computer networks to advanced concepts in ethernet networks. Extensive examples on the Windows Server 2003/2008 configuration and system configuration for Linux. Topics include denial of service attacks, firewalls, intrusion detection, password cracking, packet sniffing, and analyzing unsecured data packets, and much more.

The Art of Debugging with GDB, DDD, and Eclipse

By Norman Matloff, Peter Jay Salzman

No Starch Press, ISBN: 1593271743

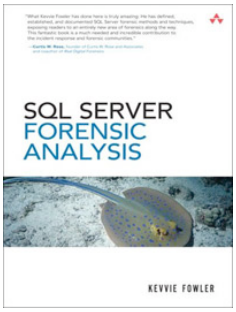


The Art of Debugging illustrates the use of three of the most popular debugging tools on Linux/Unix platforms: GDB, DDD, and Eclipse. In addition to offering specific advice for debugging with each tool, authors cover general strategies for improving the process of finding and fixing coding errors, including how to inspect variables and data structures, understand segmentation faults and core dumps, and figure out why your program crashes or throws exceptions. The book also explains how to use features like convenience variables, and artificial arrays and become familiar with ways to avoid common debugging pitfalls.

SQL Server Forensic Analysis

By Kevvie Fowler

Addison-Wesley Professional, ISBN: 0321544366

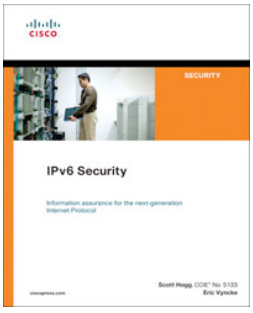


This title shows how to collect and preserve database artifacts safely and non-disruptively; analyze them to confirm or rule out database intrusions; and retrace the actions of an intruder within a database server. A chapter-length case study reinforces Fowler's techniques as he guides you through a real-world investigation from start to finish. The techniques described in the book can be used both to identify unauthorized data access and modifications and to gather the information needed to recover from an intrusion by restoring the pre-incident database state.

IPv6 Security

By Scott Hogg, Eric Vyncke

Cisco Press, ISBN: 1587055945

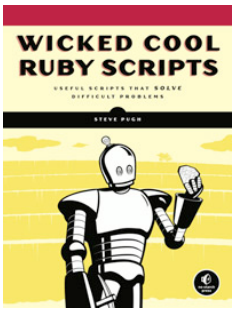


The book covers every component of today's networks, identifying specific security deficiencies that occur within IPv6 environments and demonstrating how to combat them. The authors describe best practices for identifying and resolving weaknesses as you maintain a dual stack network. You learn how to use Cisco IOS and ASA firewalls and ACLs to selectively filter IPv6 traffic. You also learn about securing hosts with Cisco Security Agent 6.0 and about securing a network with IOS routers and switches. Multiple examples are explained for Windows, Linux, FreeBSD, and Solaris hosts.

Wicked Cool Ruby Scripts: Useful Scripts that Solve Difficult Problems

By Steve Pugh

No Starch Press, ISBN: 1593271824

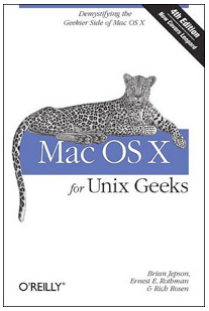


This title provides carefully selected Ruby scripts that are immediately useful. You will learn how to streamline administrative tasks like renaming files, disabling processes, and changing permissions. After you get your feet wet creating basic scripts, author will show you how to create powerful Web crawlers, security scripts, full-fledged libraries and applications, and much more. With each script you'll get the raw code followed by an explanation of how it really works, as well as instructions for how to run the script and suggestions for customizing it.

Mac OS X For Unix Geeks, 4th Edition

By Ernest Rothman, Brian Jepson, Rich Rosen

O'Reilly Media, ISBN: 059652062X

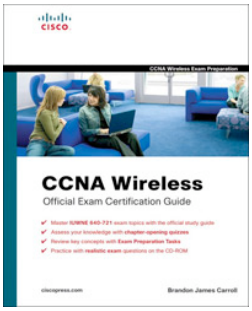


This book highlights some key differences between the Darwin environment and more conventional UNIXs, enabling people with UNIX experience to take advantage of it as they learn the Mac OS X way of doing things at the command line. This skinny volume neither aims to teach its readers UNIX nor introduce them to the Mac, but rather to show how Apple has implemented UNIX. It's a fast read that assumes--as the title implies--rather a lot of UNIX knowledge. With that requirement satisfied and this book in hand, you're likely to discover aspects of Aqua more quickly than you otherwise would have.

CCNA Wireless Official Exam Certification Guide

By Brandon James Carroll

Cisco Press, ISBN: 1587202115

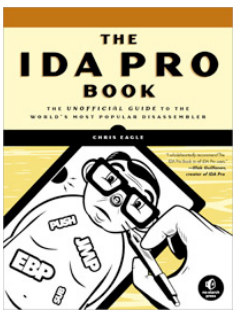


CCNA Wireless Official Exam Certification Guide is an exam study guide that focuses specifically on the objectives for the CCNA Wireless IUWNE exam. Senior instructor Brandon Carroll shares preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. “Do I Know This Already?” quizzes open each chapter and allow you to decide how much time you need to spend on each section.

The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler

By Chris Eagle

No Starch Press, ISBN: 1593271786



With The IDA Pro Book, you'll learn how to turn that mountain of mnemonics into something you can actually use. Hailed by the creator of IDA Pro as the "long-awaited" and "information-packed" guide to IDA, The IDA Pro Book covers everything from the very first steps to advanced automation techniques.

While other disassemblers slow your analysis with inflexibility, IDA invites you to customize its output for improved readability and usefulness.

2008 was a year that made many people (including security professionals), think twice about the possibility that unauthorized parties could be monitoring their Internet connection. Previously, most of us wasted no time on considering that automated software updates could lead to malware installations, or that some Certificate Authorities could be introducing fundamental weaknesses. Who would blame us? After all these years, the Internet still "worked" and the protocols remained practically the same for a long time.

During last year the media took every opportunity to describe apocalyptic scenarios regarding the future of the Internet. Various research showed that the fundamentals on which the Internet operates (eg. DNS and BGP) are flawed. That is what, alongside various incidents that had an impact on security, turned 2008 into a wake-up call. In this article I will analyze incidents and publications that made last year's security news. I will voice my thoughts on the matter and hope that those may help us with the designing of increasingly secure systems.

Fundamental Internet security flaws

Most of the security flaws that we hear about affect a specific product or system and tend to be easy to fix. On the other hand, when a protocol has a security flaw, many different products may become vulnerable. What if the vulnerable protocol happens to be part of the way that we use the Internet? I will take a look at various "discoveries" published in 2008 that show how much we over-estimate the level of Internet security.

Internet core routing protocols have weak security

As an end user, chances are you have never hear of the Border Gateway Protocol (or BGP). This is the core Internet routing protocol and one would assume that such a protocol is impervious against well known security attacks such as hijacks. However, as many of us found out when visiting YouTube in February 2008, this is definitely not true. Those on the inside knew and acknowledged that BGP had such weaknesses. For the rest of us, we learned about this the hard way when Youtube was hijacked for a few hours by a

Pakistani Telecom (tinyurl.com/cn2o7k). Later on that year, security researchers Alex Pilosov and Tony Kapela delivered a presentation at Defcon called “Stealing The Internet” (tinyurl.com/5a5nhz). During this talk they described how they had over 90% success when hijacking specific public IP addresses ranges. Anyone who is subscribed to the “North American Network Operators Group” or NANOG mailing list knows that BGP hijacks, whether accidental or intentional, occur more frequently than anyone would expect.

DNS can lie

Dan Kaminsky attempted to “patch the Internet” for a security flaw that he ran into quite by mistake. He was not trying to uncover what became the most talked about security flaw of the year, but he did. Luckily for us, his attempt to patch a large number of important DNS servers was successful. This wouldn’t have been possible without help from various important people (eg. Paul Vixie, the original writer for BIND) and organizations like Microsoft, Cisco and Sun Microsystems.

However, not only did this security flaw put into question the safety of DNS as we know it, but it also raised concerns on how well protected we are against similar issues. Many were quick to tout cryptography and PKI as the fix for these concerns. The problem is, how resistant is the public key infrastructure in the face of a DNS cache poisoning?

Late in December 2008, a team of seven security researchers and academic cryptographers showed how they were able to create a rogue Certificate Authority.

Digital certificates are not necessarily trustworthy

When certain security problems in the underlying protocols such as IP crop up, digital certificates, PKI and cryptography are seen as a remediation and a way to mitigate. For example, we rely on the security of digital certificates and the PKI to ensure that our credit card transactions are secured even though the underlying protocol (HTTP) is clear text and insecure. We make use of TLS to tunnel HTTP as a solution to that particular issue. The good thing about cryptography is that it is the only information security solution where (if done right) the attacker is at a disadvantage.

Nevertheless, during 2008, research and several incidents showed that digital certificates and Certificate Authorities were not as bullet proof as one would like to think. Servers which made use of private keys generated by Debian’s version of OpenSSL were found to be vulnerable to a major implementation flaw. The assumption with key generation is that keys are randomly generated and that the attacker cannot easily guess the private key. Debian’s version of OpenSSL was not following this rule due to a small modification in the code, that lead to the generation of a limited amount of private keys.

Late in December 2008, a team of seven security researchers and academic cryptographers (tinyurl.com/a744ng) showed how they were able to create a rogue Certificate Authority. They did this by creating two certificates with the same MD5 hash, generating what is known as a hash collision. One of the certificates was for a legitimate website that the researchers had access to. This certificate was then signed by RapidSSL (a Certificate Authority trusted by major browsers like IE and Firefox) that was at the time still making use of the vulnerable MD5 hashing algorithm.

The second certificate that the team generated (which produces the same MD5 hash) was an intermediate certificate authority cert. Since both certificates had the same hash, both would have the same digital signature issued by RapidSSL. This meant that the researchers ended up in possession of a signed and trusted certificate authority and could issue certificates for any site on the Internet of their choice. The application of such an attack varies widely. This could, for instance, allow them to perform a man in the middle attack on many HTTPS sites given that the attacker is placed between the client and server (for example, on a wireless connection).

A few days before the MD5 collision presentation, Eddy Nigg blogged (blog.startcom.org/?p=145) about how he was able to obtain a brand new digital signature for a domain name that he did not have access to: mozilla.com. He did not make use of any advanced techniques like generating MD5 collisions, but instead simply asked (and payed) for the certificate through one of Comodo's resellers (a Certificate Authority). This is not a newly discovered vulnerability; back in 2003, an issue of the 2600 magazine published an article called "Whom do you trust?" which described similar problems. It would be folly to assume that such vulnerabilities did not catch the attention of would-be criminals.

Clickjacking targets the web as we know it

Late September, Jeremiah Grossman and R. Hansen described an attack that affects a large number of websites and different modern web browsers. They named this attack "clickjacking" and it works by forcing victims to unknowingly perform actions (by clicking) on websites where they are already authenticated. This flaw could probably be seen as a user interface flaw where the end user (the victim) may think that he or she is (for example) playing a game asking you to click on a button. In the background the victim in reality might be clicking on the settings buttons in Adobe's Flash configuration. In a successful attack, this could lead to the victim giving the attacker access to the microphone and webcam. Such an attack would turn the most web browsers into a spying device. Adobe have addressed this particular vulnerability, but it is unknown at this moment how many other web browser plugins and websites are vulnerable to this attack.

CAPTCHA cracked

Once an effective anti-spam mechanism, the CAPTCHA was reduced to a mere speed bump. Not only did researchers prove that they had code that successfully detected the letters in a distorted image, but malware and spam software writers started making use of this technique in their applications. A website called captchakiller.com gives a demostration of how easy the majority of CAPTCHA systems can be broken nowadays. Major services such as Yahoo, Google and Hotmail were found to be vulnerable and the effectiveness of the CAPTCHA came into question quite a few times during 2008.

Once an effective anti-spam mechanism, the CAPTCHA was reduced to a mere speed bump.

A look at real world events

Scientology attacks

During January 2008, a video was leaked out on Youtube, showing a Church of Scientology promotional video featuring Tom Cruise. The Church allegedly tried to have the video removed from the Internet but succeeded only partially. The thing with content on the Internet is that it only takes one copy to make another.

An online community called "Anonymous" launched Denial of Service attacks on the Scientology's websites and started leaking out incriminating documents. The group started posting anti-Scientology videos on popular video sharing sites and on 2 February 2008 organized the first protest against the church. Although initially only 150 people turned up, on February 10 news reports calculated that 7,000 people protested across at least 100 cities worldwide. Some of the protesters wore Guy Fawkes masks inspired from the film "V for Vendetta".

The whole saga has to it more to it than meets the eye, but one thing is for sure: online propaganda can and does get reflected in an offline world.

Submarine cable disruption

Reliability became quite an issue in 2008 for countries in the Middle East and the Mediterranean Sea. On separate occasions in January, February and December, communications and Internet services were abruptly interrupted. The main communication channels for these countries rely on the undersea cables connecting to the rest of the world.

These cables were ripped apart by a ship's anchors, bad weather and seismic activity. Many businesses, especially those that rely exclusively on a stable Internet connection (such as the online gaming companies in Malta) were severely affected. One thing was clear: no matter how much protection you employ against traditional denial of service attacks, downtime can and does occur when the infrastructure itself is vulnerable.

Celebrities as victims

When Sarah Palin's Yahoo account was compromised, many became concerned about the security of their own webmail account. The hack was very similar to what happened to other celebrities before her (such as Paris Hilton); the "secret answer" to the password recovery question was not so secret.

The problem with being a celebrity is that many of your life's achievements and details are recorded and publicly accessible to anyone who cares to look.

A password reset page that asks for your zip code, birthday and where you met your spouse is not asking for anything that cannot be researched or intelligently guessed. It is very easy to think that such drama only happens to celebrities.

Now might be a good time to get used to the fact that our systems are not as secure or robust as we were lead to think. What was previously considered secure enough can turn out to be a security disaster the next day.

Dealing with insecurity

Now might be a good time to get used to the fact that our systems are not as secure or robust as we were lead to think. What was previously considered secure enough can turn out to be a security disaster the next day. Thanks to cybercrime, the Internet is not getting any safer. Therefore we need to handle such situations before they hit us.

It's always a good idea to think about what happens when our security systems fail. This is how "djbdns" (a DNS server) dodged the DNS cache vulnerability. DJ Bernstein (the author of "djbdns") did not rely on the security of the transaction ID (TXID, a unique ID identifying every DNS request and response) to protect his DNS server from accepting forged responses sent by an attacker.

Similarly, some sites evaded the clickjacking threat by requiring a user to confirm important actions by typing in specific information (for example a username and password). Neither of these solutions aimed to address the specific attack vectors (DNS cache poisoning and clickjacking) but were meant to protect against security vulnerabilities that could crop up when the current shields were defeated. In other words, they consisted of good application of Defense in Depth.

There are "security" systems that should be avoided all together. When setting the reset password "secret" information, one needs to make sure that the information is indeed secret. Zip codes are anything but secret, and so are details such as the first car.

My suggestion is to totally avoid answering such questions. If they are compulsory questions then filling them with information that will never be publicly associated with you and cannot be easily guessed by an attacker (randomly characters might as well do) may be a good solution.

Reliability, public relations and the Internet

The Internet has changed the way that we do business and our addiction only shines when the Internet connection goes down. The fact that the Internet does not have a central point of failure does not mean that entire countries cannot get disconnected. As much as we like to think of the Internet as reliable, this might be time to think about additional and alternative links and ways to communicate.

Online activism is not something new and if you are an organization that may become a target, then it is not an easy task to defend against such attacks. Exposure reduction can work both ways, making you less of a target but also reducing your influence.

I think that this area will be developing greatly in the coming years. We will be seeing a lot more technical attacks such as abuse of cross site scripting and SQL injection attacks to show fake articles on popular news sites, being used to subvert the masses.

Leaving it to the third party can become an issue

The hijack of Sarah Palin's "Yahoo!" account shows how depending on third party services that were not designed for the Vice President nominee is a bad idea. This does not mean that had she made use of a nonpublic mail service, her email account would not have been any safer.

However, by shifting all the security work to the hands of a third party catering for everyone, your particular security needs will probably not be addressed. Similar issues affect the idea of cloud computing, where all the data processing (hence the data) is shifted to a third party.

Theoretical and actual attacks

Many reported vulnerabilities are not fixed on the pretenses that they are simply theoretical. The researchers that demonstrated the MD5 collision vulnerability went through the trouble of acquiring over 200 PlayStation 3 consoles and working on the MD5 collisions.

Their work and time was devoted to prove that MD5 is indeed broken and should be banned from the Public Key Infrastructure. They were able to show that the vulnerability has practical implications rather than simply being a theoretical attack. This leads to the question: would attackers go through all that work to create a rogue CA? The availability of botnets for many of today's cybercrime makes the computational needs of such an attack possible. Do you see any reason why anyone would like to have access to a Certificate Authority?

Attackers will always target the path of least resistance. If they just wanted to receive a valid certificate for any site then, as Eddy Nigg and others before him demonstrated, sometimes all one has to do is simply ask for it. This vulnerability has probably been abused before for malicious motives. How can such issues not be fixed after five years?

This shows that many times nothing is fixed unless the vendors feel pressure from their customers or the software vendors (Microsoft, Mozilla etc). Motivation to solve or mitigate can only come from published research or because victim customers.

The boundary between theoretical and practical in the case of an attack is quite open to interpretation. Not knowing that active exploitation of a vulnerability is taking place does not necessarily mean that it is not affecting the end users. We would do well to start viewing vulnerability reports with a less cynical lens, accept that our systems may be flawed and making our systems more robust through Defense in Depth and other long term solutions.

Sandro Gauci is the owner and Founder of EnableSecurity (www.enablesecurity.com) where he performs R&D and security consultancy for mid-sized companies. Sandro has over 8 years experience in the security industry and is focused on analysis of security challenges and providing solutions to such threats. His passion is vulnerability research and has previously worked together with various vendors such as Microsoft and Sun to fix security holes.

Sandro is the author of the free VoIP security scanning suite SIPVicious (sipvicious.org) and can be contacted at sandro@enablesecurity.com. Read his blog at blog.enablesecurity.com

What you need to know about tokenization

by Gary Palgon

New data security model gains traction with organizations to protect sensitive information, while reducing risk and without altering applications.

As organizations seek to improve security for more types of sensitive and confidential data, data encryption and key management become more complex and resource intensive. Moving beyond simply securing payment card numbers and into guarding more diverse forms of personally identifiable information (PII), financial and IP data present new data security challenges for many enterprises - including the realization that the data resides everywhere.

It's no secret that encrypted data takes more space than cleartext data, and that many forms of PII contain many more characters than a 16-digit credit card number - all of which can pose a "square peg into a round hole" kind of storage problem with consequences that ripple through the business applications that use the data. What's more, data security professionals live and die by three profound truths. First, if you encrypt data and lose the encryption key, the data is lost forever as there is no way to get it back. Second, if you encrypt data and don't control access to the keys with equal rigor, you haven't really secured the data. Third, the fewer places you store the sensitive data, the better.

To meet the growing challenge of reducing points of risk, a new data security model - tokenization - is beginning to gain traction.

What is tokenization?

With traditional encryption, when a database or application needs to store sensitive data (for example, credit cards, national insurance

numbers, Social Security numbers), those values are first encrypted and then the cipher text is returned to the original location. With tokenization, however, rather than return encrypted data back to the originating database or application, a token, or surrogate value, is returned and stored in place of the original data. The token is then a reference to the actual cipher text, which is usually stored in a central data vault. This token can then be safely used by any file, application, database or backup medium throughout the organization, thus minimizing the risk of exposing the actual sensitive data. Because you can control the format of the token, and because the token is consistent for all instances of a particular sensitive data value, your business and analytical applications continue seamless operation.

Tokenization is an alternative data protection architecture that is ideal for some organizations' requirements. It reduces the number of points where sensitive data is stored within an enterprise, making it easier to manage and secure. A token is a surrogate value that represents, and therefore, can be used in place of the original data. Because it is a representation, it uses the same amount of storage as the original cleartext data; instead of the larger amount of storage required by encrypted data.

Moreover, because it is not mathematically derived from the original data, it is arguably safer than even exposing ciphertext (encrypted values). It can be passed around the network between applications, databases and business processes safely, all the while leaving the encrypted data it represents securely stored in a central repository. Authorized applications that need access to encrypted data can only retrieve it using a token issued from a token server, providing an extra layer of protection for sensitive information and preserving storage space at data collection points.

Tokenization enables organizations to better protect sensitive information throughout the entire enterprise by replacing it with data surrogate tokens.

For example, when a large retailer performed an internal audit, they discovered that credit card information was stored in over 200 places. Even with a strong encryption and key management solution and excellent internal procedures, the organization felt this was unmanageable and represented an unacceptable level of risk of breach. Of course, Step 1 was to get rid of the credit card information in places where it truly wasn't needed. Step 2 was to reduce the number of instances of the information to four encrypted "data silos" and substitute tokens for the credit card information in the remaining locations. This created a highly manageable architecture and reduced the risk of breach dramatically.

Referential integrity can also introduce problems where various applications (e.g. loss prevention, merchandise returns, data warehouse) and databases use the sensitive data values as foreign keys for joining tables together to run queries and to perform data analysis. When the sensitive fields are encrypted, they often impede these operations since, by definition, encryption algorithms generate random ciphertext values—this is to say that the same cleartext value (a credit card, for instance) does not always generate the same encrypted value. A consistent, format-sensitive token eliminates this issue.

Tokenization enables organizations to better protect sensitive information throughout the entire enterprise by replacing it with data surrogate tokens. Tokenization not only addresses the unanticipated complexities introduced by traditional encryption, but also can minimize the number of locations where sensitive data resides given that the ciphertext is only stored centrally. Shrinking this footprint can help organizations simplify their operations and reduce the risk of breach. Replacing encrypted data with tokens also provides a way for organizations to reduce the number of employees who can access sensitive data to minimize the scope of internal data theft risk dramatically. Under the tokenization model, only highly authorized employees have access to encrypted customer information; and even fewer employees have access to the cleartext data.

Token server in an enterprise

The most effective token servers combine tokenization with encryption, hashing and masking to deliver an intelligent and flexible data security strategy. Under the tokenization model, data that needs to be encrypted is passed to the token server where it is encrypted and stored in the central data vault. The token server then issues a token, which is placed into calling applications or databases. When an application or database needs access to the encrypted value, it makes a call to the token server using the token to request the full value.

The relationship between data and token is preserved - even when encryption keys are rotated. The data silo contains a single encrypted version of each original plaintext field. This is true even when encryption keys change over time, because there is only one instance of the encrypted value in the data silo. This means the returned tokens are always consistent whenever the same data value is encrypted throughout the enterprise. Since the token server maintains a strict one-to-one relationship between the token and data value, tokens can be used as foreign keys and referential integrity can be assured whenever the encrypted field is present across multiple data sets. And since records are only created once for each given data value (and token) within the data silo, storage space requirements are minimized.

Just like best practices for standard encryption, a best practice for the token model is to salt the digest before the data is hashed. This protects against potential dictionary attacks of the data silo to ensure the highest level of data security.

Tokenization can also minimize exposed areas when seeking compliance with mandates such as the Payment Card Industry's Data Security Standard.

Tokenization to reduce PCI DSS audit scope

Tokenization can also minimize exposed areas when seeking compliance with mandates such as the Payment Card Industry's Data Security Standard (PCI DSS). Tokenization is a powerful method for narrowing the systems, applications and procedures that are considered "in scope" for the purposes of a PCI DSS audit, providing dramatically positive implications for an organization.

When you undergo a PCI DSS audit, all of the systems, applications and processes that maintain or have access to credit card information are considered "in scope". However, if you substitute tokens for the credit card information and the systems, applications and processes never require access to the token's underlying value, then they are out of scope and do not need to comply with the PCI DSS requirements.

Because you can format tokens in any manner you wish, this enables you to, for example, render a customer service application and all of its processes as "out of scope." A typical customer service function answers billing questions and requires access to only the last four digits of a credit card number. If you format the token in this manner and do not provide the customer service applications or people with any access to the token server, then the entire function is out of scope.

The tokenization model provides medium to large enterprises with a new and more secure way to protect sensitive and confidential information from internal and external data breaches. Tokenization reduces the scope of risk, data storage requirements and changes to applications and databases, while maintaining referential integrity and streamlining the auditing process for regulatory compliance.

The higher the volumes of data and the more types of data an organization collects and protects - ranging from payment card numbers to the various types of personally identifiable information - the more valuable tokenization becomes. Fortunately, incorporating tokenization requires little more than adding a token server and a data silo.

Data encryption truths

Truth 1: If you encrypt data and lose the encryption key, the data is lost forever. There is no way to get it back.

Truth 2: If you encrypt data and don't control access to the keys, you haven't secured the data at all.

Truth 3: The fewer places you store the sensitive data, the better.

Tokenization truths

Truth 1: While field sizes increase when encrypting data; token size can follow the same size and format of the original data field.

Truth 2: Using tokens in place of actual credit card numbers or other sensitive data can reduce the scope of risk by limiting the number of places ciphertext resides.

Truth 3: Tokens can be used as indexes in key table relationships within databases, while ciphertext cannot.

Truth 4: For instances where employees do not need to see the full encrypted value, using mask-preserving token values in place of encrypted data reduces the scope of risk.

Truth 5: There is one-to-one relationship between the data value and token throughout the enterprise, preserving referential integrity.

The fewer places you store the sensitive data, the better.

Token server attributes and best practices

Tokenization provides numerous benefits to organizations that need to protect sensitive and confidential information. Fortunately, token servers that support best practices are emerging to make it easier for enterprises to implement tokenization.

Look for a token server with the following attributes:

• ***Reduces risk*** - Tokenization creates a central, protected data silo where sensitive data is encrypted and stored. Using a token server should greatly reduce the footprint where sensitive data is located and eliminate points of risk.

• ***No application modification*** - Token servers generate tokens that act as surrogates for sensitive data wherever it resides. Tokens maintain the length and format of the original data so that applications don't require modification.

• ***Referential integrity*** - Token servers enforce a strict one-to-one relationship between tokens and data values so that they can be used as foreign keys and so referential integrity can be assured whenever an encrypted field is present across multiple applications and data sets.

• ***Control and flexibility*** - The best token servers will give IT complete control of the token-generation strategy. For example, the last four digits of the data can be preserved in the token, allowing the token to support many common use-cases.

• ***Streamlines regulatory compliance*** - A token server enables organizations to narrow the scope of systems, applications and processes that need to be audited for compliance with mandates such as PCI DSS.

Gary Palgon is Vice President of Product Management for data protection software vendor nuBridges (www.nubridges.com). He is a frequent contributor to industry publications and a speaker at conferences on eBusiness security issues and solutions. Gary can be reached at gpalgon@nubridges.com.

MIS TRAINING INSTITUTE'S

INFOSEC WORLD

March 7-13, 2009, ORLANDO, FL
Disney's Coronado Springs Resort

CONFERENCE & EXPO 2009

Featuring Practitioner-Led Sessions from the Following Organizations: *(partial listing)*

American Express
Bancshares, Inc.
Bank of New York Mellon
Burton Group
Cardinal Health
Carnegie Mellon University
Coca-Cola Enterprises
Department of Veterans' Affairs
DeVry, Inc.
eBay
EMC² Corporation
General Dynamics
HSBC
Humana, Inc.
Internal Revenue Service
JPMorgan
Lockheed Martin
Macy's
Mayo Clinic
McAfee, Inc.
Memorial Sloan-Kettering Cancer Center
Merck & Co., Inc.
Michigan State University
Mitre Corp
Motorola
National Aquarium
NIST
Oak Ridge National Laboratory
PremiereTec Companies
Progressive Insurance
Prudential
Purdue University
Siemens Financial Services
Starwood Hotels and Resorts
State of California
State of Montana
State Street Bank
Stevens Institute of Technology
Susquehanna
Texas Instruments
The Nemours Foundation
The Timken Company
Towers Perrin
University of Arizona
University of Michigan
University of Nebraska at Omaha
Wachovia Corp.
ZipRealty

KEYNOTE SPEAKERS

DR. WHITFIELD DIFFIE
Vice President, Sun Fellow, Chief Security Officer, Sun Microsystems

MICHAEL T. ROCHFORD
Director, Office of Counterintelligence; Director, Field Intelligence Element, Global Initiatives Directorate, Oak Ridge National Laboratory

CISO SUMMIT CHAIR

PROF. HOWARD A. SCHMIDT
CISSP, (ISC)² *Security Strategist; former* White House Cyber Security Advisor

EARN UP TO 51 CPEs WITH THE WORLD PASS!

CO-LOCATED SUMMITS:

CISO EXECUTIVE SUMMIT, March 8
SUMMIT ON IT GOVERNANCE, RISK & COMPLIANCE, March 12
SUMMIT ON KEEPING GOVERNMENT DATA CONFIDENTIAL, March 12

www.misti.com/infosecworld

MIS TRAINING INSTITUTE
The International Leader in Audit & Information Security Training

PLATINUM SPONSORS

CISCO
websense® ESSENTIAL INFORMATION PROTECTION™

Q&A: Vincenzo Iozzo on Mac OS X security

by Mirko Zorz

Vincenzo Iozzo is a student at the Politecnico di Milano where he does some research regarding malware and IDS. He is involved in a number of open source projects, including FreeBSD due to Google Summer of Code. He also works as a security consultant for Secure Network, an Italian company, and as a reverse engineer for Zynamics. He spoke at a number of conferences including DeepSec and Black Hat.

How did you get started with Mac OS X security research?

I think at least three reasons drove me to Mac OS X related research. First of all OS X is my operating system and I usually want to have things under my control; so thinking someone could mess with my computer without being able to grasp what is going on really annoys me.

The second reason is that I don't like climbing. Since everyone said to me to start my research "on the shoulders of giants" I always tried to choose the shortest possible shoulders: definitely when I started to look into Mac OS X it was a rather new field. Finally, I was a bit surprised when I learned that almost no research was done on this OS and therefore I wanted to know why.

Can you give our readers and overview about your research process and how you search for vulnerabilities?

When I am about to start with new research I usually follow these steps:

1. I read as much as I can on the topic.
2. I try to test myself to see if I've really understood the topic.
3. I make sure that I have all the instruments I need to investigate in-depth.
4. I strongly rely on peers asking them for advice and reviews.

Eventually, when I think I've discovered something, I repeat step 1) to see if my discovery is really relevant. I must say that I usually don't search for vulnerabilities, in the sense that I am not that much interested in finding buffer overflows, XSS and so forth. In fact, I like to see if I can manage to find a technique rather than a bug to discard a system.

What's your view on the full disclosure of vulnerabilities?

Generally speaking, I prefer responsible disclosure, because it's rather pointless to expose users to needless risks. But in case vendors are hostile or do not respect deadlines, full disclosure should be applied. Whenever a vulnerability is discovered it must be patched as soon as possible and we have to assume the bad guys already know about it.

In your opinion, generally how mature is Mac OS X when it comes to security?

I think Mac OS X is well behind its competitors when it comes to security. There is a general lack of counter measures. For example ASLR is not employed for stack, heap and processes. Only the address space of libraries is randomized, but this can be easily circumvented. Further good examples are canaries - gcc version on OS X has canary support but currently applications don't employ it. By the way, rumor has it that Snow Leopard will solve these issues.

I think Mac OS X is well behind its competitors when it comes to security.

For the past year, the media has been predicting a big downfall of Mac OS X security and an onslaught of malware attacking the OS as it gains more market share. Are these fears overrated or can we really expect a security mess like the one targeting Windows?

It seems to me that everyone is willing to make predictions about information security trends. Most of the claims the media makes are overestimated, and this one is not an exception.

At the moment only a bunch of viruses are known to work on OS X, and their self-propagation ability is very low. Nonetheless, Mac OS X is a great playground for attackers as it is easier to exploit OS X than Vista or Linux.

What do you see as Apple's toughest security obstacle? What kind of possible upcoming issues should they address?

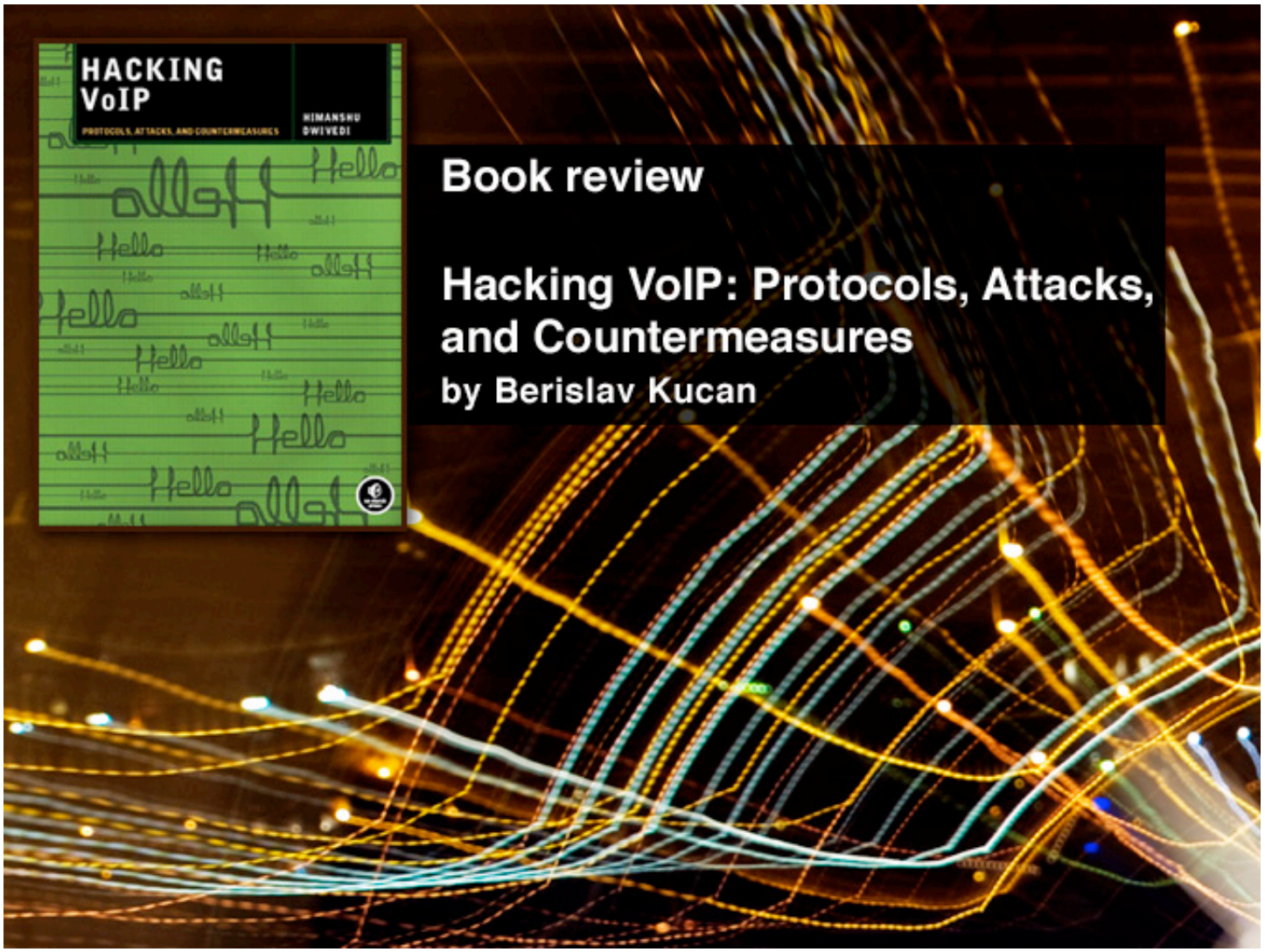
Given the current situation of OS X security, all kinds of problems that plagued other operating systems in the past can appear. I believe the most significant problem for OS X is the lack of enforcement from a security prospective of some critical applications like Safari and Quicktime. This may lead to massive client-side exploitation.

What advice would you give to Mac OS X end users that aim to make their systems as secure as possible?

First of all, they should run their system with a non administrative account, then it is a good practice to use FileVault to encrypt data and inspecting dmg files before opening them. Lastly, all security updates should be installed immediately.

What security software would you recommend to experienced users?

A lot of valid tools exist, most of them are already widely employed on UNIX. The two I appreciate most are OpenGPG and Tripwire. The former is a widely used encryption tool, whereas the latter is used to check file integrity. As a last recommendation I suggest using Systrace to sandbox critical applications or untrusted binaries.



Author: Himanshu Dwivedi | Pages: 220 | Publisher: No Starch Press | ISBN: 1593271638

Voice over Internet Protocol (VoIP) has given us an affordable alternative to telecommunications providers that were charging us a small fortune for telephone calls, especially those made to international destinations.

The average user will point out call quality as an the only possible problem in an VoIP environment, but there are numerous security issues affecting this technology and author Himanshu Dwivedi is here to dissect them for you.

About the author

Himanshu Dwivedi is a security expert and researcher. He has published four books, "Hacking Exposed: Web 2.0", "Securing Storage", "Hacker's Challenge 3" and "Implementing SSH". A founder of iSEC Partners, Himanshu manages iSEC's product development and engineering, specialized security solutions, and the creation of security testing tools for customers.

Inside the book

The popular Hacking Exposed series covered VoIP security in one of their 2006 book releases. With the advantages made in this arena, it was nice to see No Starch Press going for the same topic late last year. As you could see from the author blurb, Mr. Dwivedi co-authored some of the McGraw-Hill hacking titles and this time he takes on VoIP hacking all by himself.

The book we are featuring today is focused on discussing the major security aspects of VoIP networks - devices, software implementations and protocols. While there is a short introduction into the world of VoIP security, it is assumed that the readers are familiar with the basics of this technology, especially signaling and media protocols. In some of the chapters you will come across information of value for users of PC based VoIP implementations, but the main focus is on enterprise deployments.

As the book is full of in depth technical aspects of providing the reader with actual manifestations of VoIP security issues, I would suggest you try to follow the authors "lab setup" that he provides early into the book. He wrote down some notes on setting up a test computer with the appropriate SIP/IAX/H.323 clients and server, together with creating an attacker's workstation based on BackTrack Live CD. If you are familiar with VoIP protocols, you will be eager to see what are the things you can do better to step up the security situation in your corporate network. The author shares some quality insides about the H.323 attacks, RTP security, as well as issues with IAX.

The second part of the book tends to cover the most interesting topics - those in where the author shows actual hacking and mangling with different threat scenarios. Over about 80 pages he provides practical advice on what can get wrong and how someone can compromise the state of your VoIP security. He often uses Massimiliano Montoro's popular tool Cain & Abel to show what kind of data can be intercepted and read through your network. I particularly liked the examples on caller ID spoofing, as well as a notion of VoIP phishing that I still didn't see in real life. In the last two important chapters, the author briefly walks through methods of securing VoIP installations and provides a perfect closing with "VoIP Security Audit Program version 1.0" - a testing methodology written by himself. This valuable collection of data covers the most important audit topics, accompanied with questions and feedback results.

Final thoughts

"Hacking VoIP" is a practical guide for evaluating and testing VoIP implementation in your enterprise. I liked the concept where the author focused just on "upper scale" deployments, making the book perfect for the system administrators that are getting deeper into the world of securing VoIP.

Here are some of the Twitter feeds we follow closely and can recommend to anyone interested in learning more about security, as well as engaging in interesting conversations on the subject. Our favorites for this issue are:

@jeremiahg
Founder and CTO of WhiteHat Security
http://twitter.com/jeremiahg

@security4all
Security blogger
http://twitter.com/security4all

@lbhuston
Security Evangelist and CEO of MicroSolved
http://twitter.com/lbhuston

@lennyzeltser
Leads a regional security consulting team at Savvis
http://twitter.com/lennyzeltser

@pauldotcom
PaulDotCom podcast and blog
http://twitter.com/pauldotcom

If you want to suggest an account to be added to this list, send a message to **@helpnetsecurity** on Twitter.

A framework for quantitative privacy measurement

by Aaron D. Sanders

Defining and measuring privacy are two topics that have produced varied results. Studies have measured consumer reaction to privacy issues and the relationship between privacy and consumer behavior. However, few studies have attempted to empower consumers to make informed decisions regarding the privacy protections provided by goods and services, or to measure the "privacy level", which is the amount of privacy in their environment. This article defines privacy and sets forth criteria for privacy measurement. It discusses a framework for quantitative privacy measurement, and introduces tools that individuals can use to conduct their own privacy measurements. The article's conclusion discusses areas for further research.

Defining privacy

In a little more than a century, the term "privacy" has acquired many definitions. In his 1879 book entitled A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract, Thomas M. Cooley provided one of the most cited definitions, when he called privacy "the right to be left alone". In their 1890 article in the Harvard Law Review entitled The Right to Privacy, Samuel Warren and Louis D. Brandeis described privacy as a legally protected right, and provided another oft-cited phrase, "the right to privacy". Dictionary.com lists three dictionaries that have six different definitions for privacy (dictionary.reference.com/browse/privacy).

In his 2002 article in the Journal of Business Ethics entitled Electronic Monitoring and Privacy Issues in Business-Marketing: The Ethics of the DoubleClick Experience, Darren Charters stated that no one definition of privacy applies to every situation, and that a number of acceptable definitions exist.

He discussed three main definitions of privacy: The right to be left alone, the right to control access to one's personal information and the right to withhold certain facts from public knowledge. In their 2003 article in the Journal of Business Ethics entitled Some Problems with Employee Monitoring, Kirsten Martin and Edward Freeman discussed "control theory" and "restricted access theory". Alan Westin (Privacy and Freedom, 1967), Charles Fried (Privacy, The Yale Law Journal, 1968) and Aaron D. Sanders (Public Policy and Technology: Advancing Civilization at the Expense of Individual Privacy, Rochester Institute of Technology MS Thesis, 2006) discussed the "control" aspect of privacy.

This article selects "control" as the definition of privacy. Ultimately, individuals have varied beliefs regarding the amount of information they are willing to share, and with whom. Secretive behavior and information hiding is not required in order to maintain a sense of privacy. Rather, individuals require control over the breadth and scope of information sharing. Some individuals may desire to keep every aspect of their existence secret, and others may opt to share their information freely.

Social networking sites such as MySpace and Facebook provide examples of the entire spectrum of information sharing possibilities, from simplistic and falsified entries to pictorial displays that threaten the safety of the depicted individuals. The definition of privacy is satisfied if each individual can control the selection of shared information to the extent desired.

ULTIMATELY, INDIVIDUALS HAVE VARIED BELIEFS REGARDING THE AMOUNT OF INFORMATION THEY ARE WILLING TO SHARE, AND WITH WHOM

Measuring privacy

Most academic studies attempting to measure privacy have focused on the effects of some aspect of privacy on consumer behavior and information sharing (for further research, the works of Glen Nowak, Joseph Phelps, Elizabeth Ferrell and Shena Mitchell provide a good starting point). While these studies have provided data on consumer behavior for organizations to consider when developing products, services and associated marketing campaigns, they were focused on the producer and not the consumer.

Recently, academic papers have focused on the use of technology for protecting privacy during a given process and measuring the amount of its loss (for further research, the works of Elisa Bertino, Igor Nai Fovino & Loredana Parasiliti Provenza or Alexandre Evfimievski, Johannes Gehrke & Ramakrishnan Srikant provide a starting point).

While these papers have created theories and processes that companies could integrate into future products, they have not provided individuals with tools to protect their privacy or conduct privacy measurement.

Numerous court cases have resulted in a decision that measured privacy's scope. In R v. M (M.R.) [1998] 3 S.C.R. 393, the Supreme Court of Canada ruled that students have a diminished expectation of privacy in a school setting compared to other situations. In that case, the Court found that a diminished expectation of privacy is reasonable, because teachers and administrators have the unique task of providing a safe environment, and because students are informed in advance that searches may occur (M.R. 3 S.C.R at 396).

The Justices cited numerous previous cases, and I encourage the review of its transcript, available from tinyurl.com/c9pler. In the opinion for Griswold v. Connecticut, 381 U.S. 479 (1965), United States Supreme Court Associate Justice William Douglas wrote that the United States Bill of Rights guarantees a "right to privacy" and a "zone of privacy" through penumbras from the First, Third, Fourth, Fifth and Ninth Amendments (Griswold 381 U.S. at 483-86). This was a landmark case in measuring individual privacy, and was followed by other similar decisions regarding an individual's body, sexual activity and the privacy of their home, most notably Eisenstadt v. Baird, 405 U.S. 438 (1972); Roe v. Wade, 410 U.S. 113 (1973); Lawrence v. Texas, 539 U.S. 558 (2003).

Another landmark case for measuring the scope of privacy was Katz v. United States, 389 U.S. 347 (1967). In the opinion, Associate Justice Potter Stewart wrote, "For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection… But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected" (Katz 389 U.S. at 351). In his concurrence, Associate Justice John Marshall Harlan II wrote that the United States Constitution protects a "reasonable expectation of privacy" if a) an individual exhibits an expectation of privacy and b) society is prepared to recognize that expectation as "reasonable" (Katz 389 U.S. at 361). Scholars named those points "Harlan's Test" for determining whether a situation warranted an expectation of privacy. The discussed cases have measured the scope of privacy, but have not measured privacy as a quantitative value.

In the Information Technology (IT) field, an increased focus on information security and compliance has led to the development of numerous products that can test systems and applications for known security vulnerabilities and improper configurations. These products can test for technical issues that might reduce privacy, but they cannot make judgments on the information collection and sharing of any given application or service. Additionally, these products are cost prohibitive to individual users.

A few works have focused on quantitative privacy measurement. In 2006, Privacy International (PI), in conjunction with the Electronic Privacy Information Center (EPIC), published the inaugural international privacy rankings. The rankings, drawn from their annual Privacy & Human Rights Report, judged 36 countries based on 13 criteria. The countries were then scored on a scale of 1 to 5 (5 being the highest) in each category. In 2006, I created the Privacy Level Indicator (PLI) in an attempt to quantitatively measure the "level of privacy".

The PLI was designed to measure privacy as the "level of privacy as it should affect all individuals". My research was an extension of similar efforts by EPIC. The PLI was designed to measure aspects of the "privacy environment" or the "current privacy conditions," and enabled measuring the effects of individual events on the level of privacy. These initiatives advanced quantitative privacy measurement, but the efforts were at the global level, and were not focused on individuals.

Framework definition

We have seen that privacy is an objective term, and difficulty exists in quantitatively measuring an objective value. While considering the topic of privacy measurement, I developed the Privacy Measurement Framework (PMF).

The PMF is designed to enable individuals to measure the privacy level of their environment, and to measure the level of privacy provided by any given product or service.

The PMF is an extension of the PLI, my initial attempt at privacy measurement. The PLI is very rigid, and is designed to measure privacy as if it were a singular universal entity. The PMF acknowledges that individuals vary in their definition and requirements for privacy, and provides them with tools for making informed measurements.

In software development, the core job of any framework is to provide a skeletal support system for completing a task. A framework specifies a base set of components, but also enables users to add additional components not included in the original framework specification. One singular tool cannot serve as a method for quantitative privacy measurement for every individual and every potential product or service. However, with a framework model, the potential number of tools is unlimited. The next section applies framework concepts to the PMF.

Framework Requirements

The PMF must be customizable. One of the main reasons for creating any framework is to enable the creation of additional components. The PMF must enable users to add, remove or customize components to suit their own expectation of privacy. The PMF must be flexible. It must be useful in measuring a wide variety of products and services, and be able to suit each individual's varying privacy requirements. A rigid design will prevent users from changing its components.

The PMF must be granular. It must have the ability to evaluate the smallest risks to individual privacy and provide a thorough analysis of all products and services.

The PMF must be intuitive. Its design and documentation must enable a short adoption time for all users. The PMF will not be widely implemented if users do not understand its application, necessity or purpose.

The PMF must be descriptive. It must provide ample feedback to users describing the results of their analysis. The PMF is a tool for creating better-informed individuals, and it must go beyond providing simple numerical results.

The PMF must be thorough. It must be each user's first and last resource. It must provide results that are convincing and completely satisfy their needs.

Framework components

Every framework requires a set of initial components, to enable users to begin working immediately. The PMF includes two components: The PLI and a Privacy Measurement Checklist (PMC).

Originally, I developed the PLI as a tool for measuring the level of privacy as it affects all individuals, and defined five levels of privacy:

1 - Controlled
2 - Acceptable
3 - Uncomfortable
4 - Threatened
5 - Uncontrolled.

The PLI has quarter points between each integer value, for added granularity. I believe that I (and others before me, including EPIC and PI) were correct in attempting to quantitatively measure privacy. However, it is important to supplement a universal measurement with individual measurements. The PMF includes the PLI, but changes its focus from universal measurements to individual measurements.

Individuals would arrive at their privacy measurement by drawing from information gathered from news sources, and applying their worldview and opinions to that information. For example, when the USA PATRIOT ACT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism; Public Law 107-56) was passed, an individual that is uncomfortable with providing the government with unrestricted surveillance powers might raise their PLI to 4.25.

An individual that supports expanding the government's surveillance powers might only raise their PLI to 2. As the PLI is measuring the "privacy climate", it is similar to a thermometer, and does not lower its measurement of the privacy level until conditions change. Other government programs, such as TIA (Total Information Awareness), MATRIX (Multistate Anti-Terrorism Information Exchange) or CAPPS II (Computer Assisted Passenger Prescreening System) could cause a user to raise their PLI. Positive changes in the privacy environment, such as the cancellation of the previously mentioned programs or the repealing of selected clauses in the PATRIOT ACT could cause users to lower their measurement.

The user's worldview and desire for privacy dictate the change decision and change delta. The next section discusses the PMC, which enables individuals to measure the privacy of products and services.

The PMC enables measuring the privacy protections in products and services. Table 1 shows the initial PMC for a Web-based application. The PMC contains items that protect individual privacy, categorized by type. Users assign a weight to each item as a portion of 100%. They choose the respective value for each item by determining how important that item is to them. The sum of the values from all sections must equal 100%. Not every product or service will require values in all sections or for all items.

Sections or items that do not apply are not assigned a value. After assigning the percentages, users would determine whether the product or service satisfies each item. Satisfied items receive a score equal to the assigned weight. Unsatisfied items receive a score of "0". The user sums the scores, and based on the total score, makes a determination on the level of privacy provided by the product or service.

The PMC includes a suggested scoring breakdown: 0-25% is “Low” privacy protection; 25%-50% is “Moderate (Low)” privacy protection; 50%-75% is “Moderate (High)” privacy protection; 75-100% is “High” privacy protection.

Table 1: Privacy Measurement Checklist version 1.0 – 2009

1) **Technical Checks**
   a. Uses Secure Sockets Layer (SSL)
   b. Personal information encrypted in storage
   c. Information encrypted on backup tapes
   d. Does not participate in advertising networks or set tracking cookies
   e. Personal information encrypted in cookies
   f. Does not use Web beacons
2) **Operations Checks**
   a. Only stores name (full or partial) if necessary
   b. Only stores full address if necessary
   c. Stores only Zip Code or state
   d. Only stores age if necessary
   e. Only stores full phone number if necessary
   f. Only stores area code
   g. Only stores eMail address if necessary
   h. Does not store Social Security Number
   i. Does not store credit card or bank account information
3) **Legal and Policy Checks**
   a. Complies with Safe Harbor
   b. Complies with FERPA
   c. Complies with HIPAA
   d. Complies with PCI DSS
   e. Complies with ISO 27001:2005
   f. Displays a privacy policy
   g. Displays known seals from TRUSTe or other organizations
   h. Has no or few known complaints against it in the news or Better Business Bureau
   i. Complaints are resolved in a timely manner

Table 2: Privacy Measurement Example

ITEM	WEIGHT	PASSED?	SCORE
1. Technical checks			
a) Uses Secure Sockets Layer (SSL)	40%	Yes	40%
b) Personal information encrypted in storage	20%	Yes	20%
c) Information encrypted on backup tapes	20%	No	0%
d) Does not participate in advertising networks or set tracking cookies	10%	No	0%
e) Personal information encrypted in cookies	10%	No	0%
Totals	100%		**60%**

The PMC is completely customizable, and users can add items to each section, or adjust the final scoring ranges to suit their desire for privacy.

Next, we will examine the PMC and show an example of privacy measurement using the PMC.

Table 2 displays an example privacy measurement using the PMC for a product or service that only requires technical checks.

In this example, the product or service (a Web-based application) scored 60%, which is the "Moderate (High)" category, according to the default scoring ranges. The user would decide whether the product or service provides satisfactory privacy protection, or whether they need to find one that scores higher, or meets specific items. Users who feel uninformed regarding the items on the PMC could ask someone to assist them or complete the scoring for them. Users could present the PMC to a representative from the product or service under examination, similar to an RFI (Request for Information) or RFP (Request for Proposal) used in most corporate bid processes.

Conclusion and further research

The primary purpose of this article is to advance research into quantitative privacy measurement, and to provide individuals with tools for conducting privacy measurements. It selected a definition for the term privacy, defined the measurement criteria and discussed a PMF for quantitative privacy measurement. The article discussed the PMF requirements and initial tools, and provided examples of using the PMF for privacy measurements. Individuals can use the PMF for measuring the privacy level of products, services and the privacy level.

Further research must involve actual users. Tools are only useful if they gain the approval of the target audience. Users must test the PMF components and add their own tools and measurement criteria. The PMF is designed to empower individuals to perform their own privacy measurements, and make informed decisions regarding products and services. If the PMF is not useful, then it will have failed its purpose. With proper user testing, the PMF will assist its users in protecting their desired level of privacy. An important component of the user testing will be to determine whether users are able to understand the tools and adopt them for their desired purposes. A significant portion of current security and privacy research focuses on user awareness training. Many users, especially personal users, do not fully understand privacy risks and the protections available.

One core role of the PMF is to allow individuals to perform risk assessments of products and services. Further research must broaden the PMF's focus, to allow it to provide general information security measurements, in addition to privacy measurements. This research should also examine whether the PMF can apply to areas not directly related to information and technology, such as physical security. Part of this research should include an examination of the requirement differences between home users and professional users. A more encompassing framework could be very beneficial for business professionals when reviewing RFI/RFP documents.

Ultimately, I hoped that this article would generate discussion on quantitative privacy measurement. One person cannot have all of the answers. This is especially true when dealing with privacy, which affects everyone differently. I hope that this article causes others to consider this topic, especially if they believe they have a better approach than mine.

Aaron D. Sanders is an Organization Information Security Manager for Xerox Global Services in Rochester, New York. He guides the security and privacy initiatives for a Web application development environment and a Software as a Service (SaaS) hosting environment. His responsibilities include implementing a secure development lifecycle, conducting Web application security tests and implementing security controls in the hosting environment. He holds a B.S. in Information Systems from Clarion University of Pennsylvania and a M.S. in Information Technology from Rochester Institute of Technology, where his thesis studied the effects of technology and public policy on individual privacy. He can be reached at aaron.sanders2@xerox.com.

GFi MailSecurity

Complete email security with up to five anti-virus engines for Exchange/SMTP/Lotus

No single anti-virus vendor scanner is the BEST and can stop ALL viruses. To obtain maximum security, you need GFI MailSecurity which uses not one, but up to five virus scanners to check all company email, with limited or no effect on network and server performance.

GFI MailSecurity is better priced than most single anti-virus engine solutions on the market. With multiple anti-virus engines you:

- React fastest to the latest virus threats by receiving the quickest virus signature updates
- Take advantage of all their strengths because no single anti-virus scanner is the BEST
- Virtually eliminate the chances of an infection.

Kaspersky Anti-Virus
McAfee
NORMAN
bitdefender secure your every bit
AVG Anti-Virus

Download your FREE trial version from www.gfi.com/ehns/

GFi NETWORK SECURITY
CONTENT SECURITY
MESSAGING

tel: +1 (888) 243-4329 / +1 (919) 379-3397 | fax: +1 (919) 379-3402 | email: sales@gfiusa.com | url: www.gfi.com/ehns/

With shrinking IT budgets and growing data storage demands, IT professionals are faced with quite a conundrum in the New Year. Virtualization technology, which offers an economical alternative to investing in additional physical storage space, has never looked more appealing.

A recently released benchmark research report by Aberdeen Group called "Virtual Vigilance: Managing Application Performance in Virtual Environments" revealed that organizations conducting server, desktop, and storage virtualization projects are experiencing 18% reductions in infrastructure cost and 15% savings in utility cost.

Not surprisingly, industry experts are almost unanimously predicting that 2009 will usher in a new age in IT spending, one where virtual service and product providers will rake in a substantial percentage of total spending, and perhaps, contend with investments in the physical storage arena. Gartner has even forecast that more than 4 million virtual machines (VMs) will be installed on x86 servers this year, and the number of virtualized desktops could grow from less than 5 million in 2007 to 660 million by 2011.

But this migration away from physical storage is fraught with mounting concern. As more and more critical business functions are being performed in virtual environments, system downtime has increasingly broader and more devastating implications for businesses—both in terms of lost revenue and customer dissatisfaction. With just one major system failure, the significant cost-savings associated with implementing virtual technology disappear and IT is left with a serious mess to clean up.

The fallibility of virtual server systems makes sense. When businesses replace multiple physical servers with virtual machines that rely on one physical machine, the hypervisor and the physical server on which it runs become a single point of failure. Enterprises are essentially placing all their eggs in one basket. Creating such vulnerability decreases the availability of applications and their data. Ultimately, it increases the risk of downtime.

Planned and unplanned downtime

System downtime is often planned, such as when a business performs necessary software upgrades or hardware maintenance.

It can also be unplanned, due to power outages, natural disasters, and more likely, software, hardware and network failures. By most accounts, both planned and unplanned downtime of some sort is unavoidable.

Given the apparent certainty of downtime, how can IT professionals effectively account for the single points of failure created by virtual server environments? One method is to employ real-time, server-level data replication across their enterprise systems. This type of replication technology offers a higher level of protection and data availability than ordinary backup strategies (although, implementing it alone does not eliminate the need for backups for archival purposes and to protect against accidental deletion of data).

With real-time, server-level data replication technology in place, IT professionals can all but eliminate the negative effects of planned downtime. Data replication allows them to switch applications over to a backup server prior to the primary system being taken down for maintenance or other purposes. Best of all, if the failover procedure is automated, application downtime is often virtually unnoticed by users.

Because it can be performed in either the host OS or the guest virtual machines, real-time, server-level data replication also provides system administrators with the flexibility to choose which VMs and applications are replicated, and which are not. When replication occurs within the guest VM, administrators have granular control over exactly which data is being replicated and when. Conversely, if most or all applications and VMs need to be replicated, then replicating entire VM images (or the entire VM image store) from the host OS level leads to a much simpler configuration - where only one replication job needs to be created and managed in order to replicate all the VMs on a given host.

GIVEN THE APPARENT CERTAINTY OF DOWNTIME, HOW CAN IT PROFESSIONALS EFFECTIVELY ACCOUNT FOR THE SINGLE POINTS OF FAILURE CREATED BY VIRTUAL SERVER ENVIRONMENTS?

Putting it in context

Take, for example, the small business that wants to protect two VMs on one physical machine if unforeseen disaster strikes. The VMs are each hosting a database that contains mission-critical data. The information is programmed to replicate over a T1 line to a remote disaster recovery site at a hosted facility.

Due to bandwidth limitations, however, only a few gigabytes of data can be replicated at one time. IT opts to replicate within the guest VM and ensures that only the volumes containing the databases and database log files are copied in real time. The other data, such as configuration data, system logs, and the OS itself, are not critical and can be re-generated from other sources, if necessary.

On the other end of the spectrum, an enterprise with a large cluster of eight physical machines hosting forty VMs wants to replicate data to a remote office for disaster recovery purposes. IT at this enterprise, however, has a gigabit link to the remote site. So for ease of administration, IT chooses to replicate at the host-level, replicating the entire VM image store (containing all 40 VMs) with a single replication job. If IT had chosen to replicate inside the VMs themselves, at the guest-level, at least 40 replication jobs would need to be configured and monitored—resulting in an hefty amount of wasted IT time and resources.

In both scenarios, efficient replication in virtual environments is of primary importance. It dictates the constraints that will be place on network bandwidth and plays a significant role in determining whether or not to replicate on the guest- or host-level. For large or small businesses that want to replicate across WAN environments, where bandwidth is especially precious, efficient replication is even more vital. Ultimately, efficiency helps IT to effectively meet its disaster recovery goals.

Implementing efficient replication

IT professionals have three primary considerations when it comes to efficiency.

The first step is to determine, or measure, the available network bandwidth within the business. The rate of change of the data - or the amount written to disk during a specific time period - must then fit within that window of network availability (the rate of change of data can be measured on most platforms using various system monitoring tools).

Next, IT must carefully choose which VMs and applications need to be replicated to get the business up and running again. If an entire VM image copy is not desired, such as in the small-business example mentioned above, IT professionals can opt for the real-time replication of only the volumes containing the databases and database log files. During peak business hours when the available network bandwidth is lower, it's less critical to replicate the other data, such as configuration data, system logs, and the OS. Instead, this additional information can be replicated during off-peak hours.

Finally, the use of compression can dramatically reduce bandwidth usage, often achieving a 2:1 reduction. With data de-duplication, defined as the process through which redundant data is eliminated so that only the unique data is stored, network compression ratios can be even higher. Compression is particularly useful for replicating over low bandwidth WAN connections, which otherwise may not support the traffic generated by an active VM.

VIRTUALIZATION IS ONLY AS SUCCESSFUL AS ITS SECURITY.

Don't overlook CDP

While not directly related to replication optimization, continuous data protection (CDP) capabilities also offer IT professionals a higher level of data protection when implementing disaster recovery technology. CDP logs all changes that occur and enables time-specific rollbacks to any point preceding an unplanned event, or disaster.

Additionally, CDP is particularly useful in protecting against accidental deletion of data or from corruption due to hardware or software bugs. Together, data replication and CDP enables IT to quickly restore business processes and maintain continuity as well as contain the permanent damage caused by unforeseen downtime and investigate and repair its source.

Leading market analyst firms such as Forrester, IDC, Gartner, Enterprise Strategy Group and Yankee Group are all reporting that virtual machines currently used by at least 75 percent of all IT systems. Now is the time to effectively implement disaster recovery planning practices and technologies. In order to maintain the true cost-savings associated with virtualization, IT professionals simply have no other choice. Virtualization is only as successful as its security. Employing real-time, server-level data replication and CDP rewind capabilities gives IT professionals the tools to secure their virtual investments and prepare for both planned and unplanned downtime.

Paul Clements is a lead software architect at SteelEye Technology, Inc. (www.steeleye.com), where he focuses on kernel- and system-level programming for data replication, high-availability and storage purposes. With over 10 years of professional experience in software engineering, he has worked on a wide array of projects on Linux, Windows and UNIX platforms.

In his personal life, Paul is an avid Linux user, developer and enthusiast. He discovered the platform back in 1995 and has since contributed to several open source projects, including the Linux kernel, of which he is the current maintainer of the Network Block Device (NBD) driver. Paul holds an MS in Computer Science from the University of South Carolina.

Q&A: Scott Henderson on the Chinese underground

by Mirko Zorz

Scott Henderson is a retired US Army analyst who served in the intelligence community for 20 years as a Chinese linguist. He holds a Bachelor of Science degree with an emphasis on Chinese studies and he graduated from the Defense Language Institute in Monterey California. He maintains The Dark Visitor blog at www.thedarkvisitor.com

How did you get interested in the Chinese underground?

In 2006, I attended the XCon2006 computer security seminar held in Beijing China and in 1997 was on special assignment to the US Embassy in the People's Republic of China. One of my fondest memories was attending the Beijing Institute of Economic Management Immersion Program in 1995.

My reason for trying to locate and study the Red Hacker Alliance oddly enough came from the headlines announcing its disbandment. It was impossible to believe that this large organization, with such an extensive history, could simply disappear overnight. The group must still be around; in what shape or form it was impossible to tell but surely it continued to function in some capacity. Initially the idea for this project was far less ambitious. The hope was to find Chinese citizens on the web talking about the alliance or Chinese news articles that had not found their way into Western press. Then, if their ongoing operations were confirmed, publish an article reporting those findings. What was ultimately uncovered was an extensive, well-organized, online community made up of 250+ Chinese hacker web sites.

Essentially, how does the world of Chinese hackers differ from other such communities around the globe? What makes it unique?

One of the unique aspects of the Chinese hacker organization is their nationalism, which is in stark contrast to the loner/anarchist culture many associate with the stereotypical Western hacker. They are especially active during periods of political conflict with other nations and until very recently have maintained a strict code of never hacking inside

China.

Their sense of patriotism in defending their national honor and their stringent codes have helped bolster their reputation among the Chinese people and aided in recruiting thousands of members. Indeed, a strong argument can be made that it was political activism that initially brought the group together.

They specialize in attacking online gaming sites and the resale of virtual property. Writing Trojans such as Gray Pigeon and Glacier is a part of the Chinese hacker culture. They actually have pride in their indigenously produced programs.

What are the most significant problem facing the Chinese cyber world?

In terms of security, everything. There are 290 million people online, along with 50 million bloggers that have limited knowledge of computer security. They own a cyber community with somewhere in the neighborhood of 300,000 hackers. Estimates run as high as 85% of all Chinese computers are infected with one type of virus or the other. The place is a mess.

Having said that, it is also a wonderful, untamed place that seems to be bursting with life and opportunity. Sort of the Wild-West of cyber space.

Writing Trojans such as Gray Pigeon and Glacier is a part of the Chinese hacker culture. They actually have pride in their indigenously produced programs.

How effective is law enforcement in China in regards to cyber crime? Does the punishment fit the crime?

The Chinese freely admit that their national law is inadequate to cope with the current state of the internet, more specifically internet crime. Until recently, it didn't even address, in a meaningful way, what constituted an online violation.

The legislature is currently trying to work through this and it is moving up the ladder in terms of priority but only domestically. There is a branch in the Ministry of Public Security called the "Cyber Police" that has cracked some internal criminal cases, made them very public but nothing significant. Most people outside of China consider the cyber police to be a form internal monitoring and censorship. Probably true but the Chinese hacker community is starting to turn on its own people and Beijing has to find a way to bring it under control.

China just recently stiffened the penalties for conviction from around 1-3 years to a maximum of 7 years for online criminal offenses. Considering the lawless nature of their online community, I would probably come down on the side of too lenient. Of course you have to consider in the nature of the crime and how actual enforcement of the existing code would affect behavior.

How big are identity theft and malicious code attacks in China? What trends can be observed in comparison to the rest of the world?

While Chinese hackers don't specialize in it, identity theft will undoubtedly become more pronounced as disposable income inside the country increases. In 2007, the Shenzhen police busted a ring of 18 people who had made off with around USD $13 million. They were working some kind of speedy loan angle to con people into giving up their information.

They are probably behind the rest of the world in relation to identity theft but it is only due to the environment and the fact they have found the niche of stealing virtual identities very profitable. I imagine the online gaming community would strongly disagree with me on my assessment of their ability to steal identities.

In your opinion, what are the events that defined the past year in the Chinese underground? What can we expect in 2009?

1. The refinement of the hacker "virus chain." Chinese hackers have been breaking into groups of around 6-10 members who write, disseminate, launder and sell virtual items. While not as exciting as breaking into the White House, this marks the point they have entered organized crime. It's no longer free-wheeling kids, these are organized, professional criminals.

2. Increased attacks on India. Whenever you have two nuclear armed neighbors ratcheting up hostilities, for whatever reason, it is a cause of concern. I haven't personally monitored any of these attacks but reports coming from inside India indicate it is becoming tiresome.

3. Increased attacks inside China. In the past it was unwritten law that you did not hack inside the country. That "unwritten" law is now a thing of the past and we have seen hundreds of internal attacks. This could possibly force a showdown between the Chinese hacking groups and Beijing. A battle they will lose.

4. Hitting financial institutions. While the political hacking makes blaring headlines, the financial attacks we've seen worry me the most; the reports of Chinese hackers breaking into the World Bank and the International Monetary Fund. Nothing really new for hackers, especially the Russians but certainly something to keep an eye on.

In the past it was unwritten law that you did not hack inside the country. That "unwritten" law is now a thing of the past and we have seen hundreds of internal attacks.

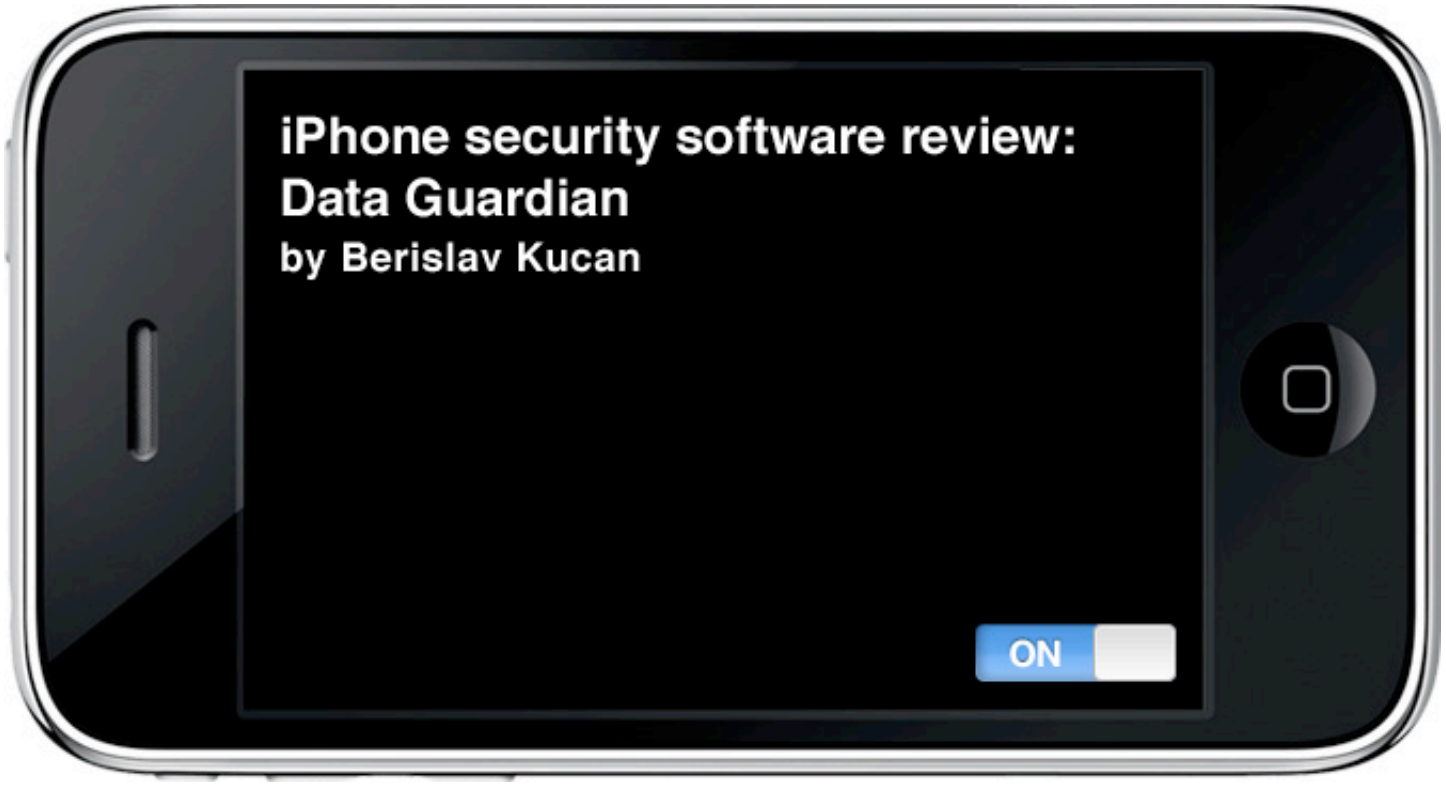
For 2009, I hate to make predictions, so we will call this a forecast:

1. Financial institutions, energy and research and development organizations will be targeted more heavily.

2. Tensions and pressure will increase between Beijing and the hacker community.

3. We will see solid evidence of cyber alliances between groups such as the Red Hackers, Russian Business Men, Pakistani, etc. We may also witness wars against each other. Certainly some people make a good case that these things have already taken place.

4. The Kappa Girl video will remain the most popular post on my website even if I discover that Chinese hackers have seized control of the US government.

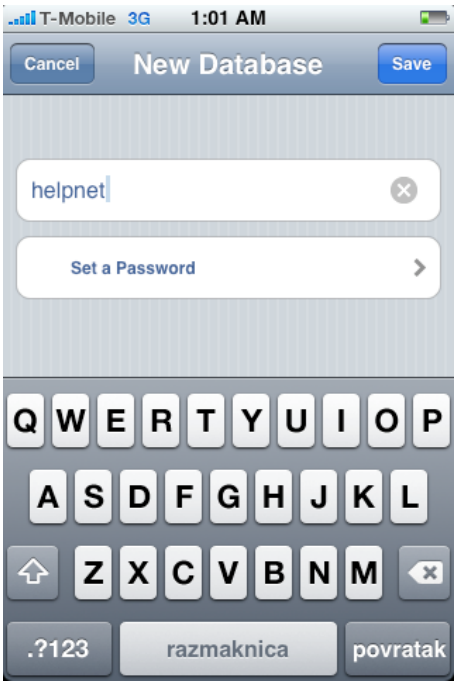


Koingo Software is a developer of various applications for multiple platforms including Windows, Mac OS X and now the iPhone. For quite some time our download section hosts their flagship security utility Data Guardian for both the Mac and Windows.

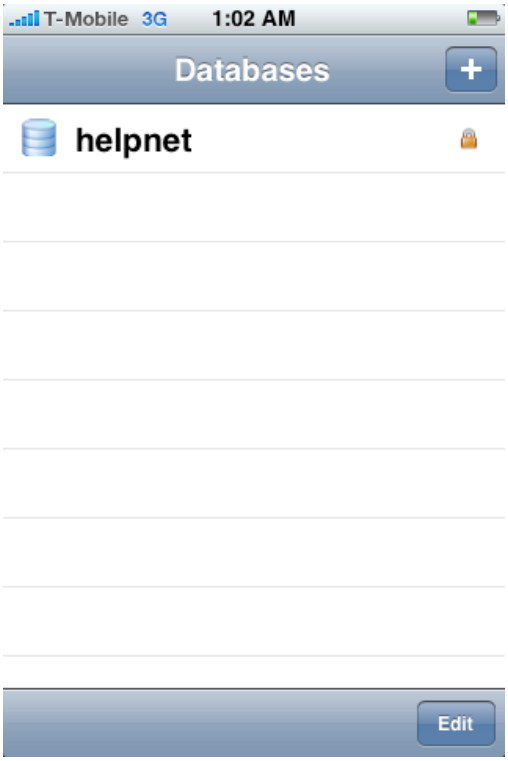
Last month Koingo announced that they have ported the Data Guardian technology to the iPhone and I bought it as soon as the software was approved for placement in the App Store. The version I tested is 1.0.1 and it goes for $1.99.

Data Guardian is a security utility that allows you to hold all your private information inside a locked database. While there are numerous similar products for multiple platforms, I really liked the way Data Guardian users are empowered to create their own specific sets of information holders.

As you will see later in the text, the user has an unique ability to fully customize the database for her own use.

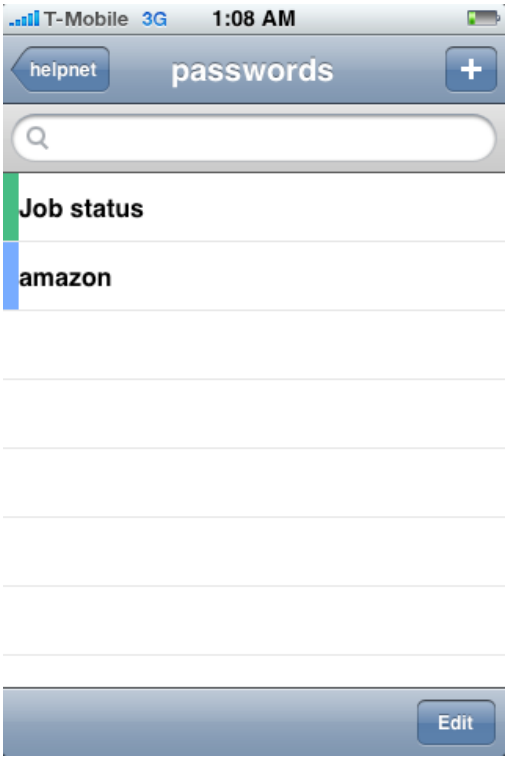


The first thing to do is to create your database and equip it with a password that will make you input and use your private information.

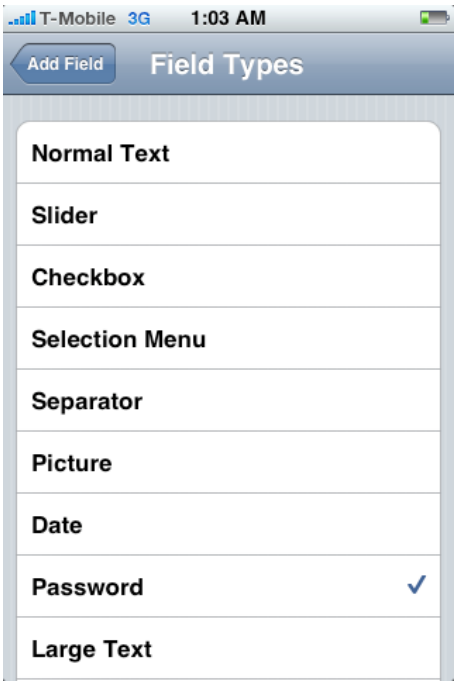


After opening a database, you are provided with two predefined information holders - the Library and a stack for unfilled data. Besides these, from the obvious usability perspective you should create your own collections where you can host specific sets of information - job related, personal, banking, passwords etc. The data structure inside Data Guardian is constructed as follows:

database > collection > records > information



When creating a record, the user has full power over the type of data it will hold. As you can see from the screenshot below, you can set some of the usual field types such as a text box, data and password, but for more advanced use, you can also find checkbox, slider (with 0-100% range), multiple choice menus, as well as a large text box. The latter provides Notepad functionality inside the locked Data Guardian database.



Getting around record customization will take a bit of your time, but as soon as you get familiar with the concept, you will create specific information sets quickly.

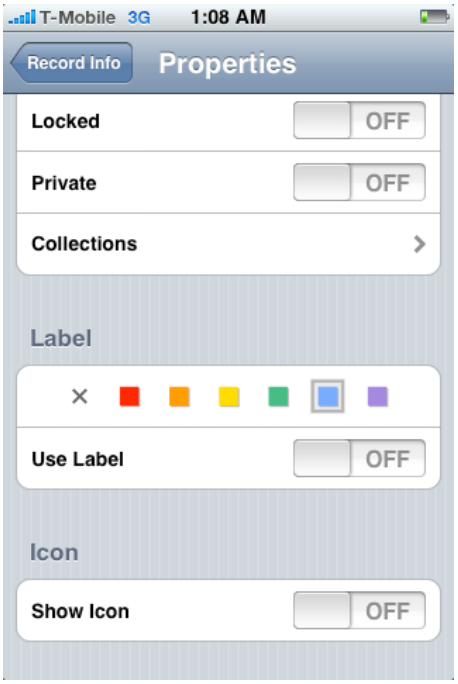
To make things easy, every record set you create can be saved as a predefined template which is handy with larger databases.

When creating lists of contacts, you will most probably use phone and e-mail fields. The phone field can store phone numbers in different formats and the "live results" will be active in a way that clicking a number inside Data Guardian will automatically call the person in question.

In this situation, after the call you will need to re-authenticate to the applications. Unfortunately, the e-mail field does not use the same automatic usage functionality.

There is a bug that didn't give me an option to move the cursor to a specific place in the e-mail address field. To change the content, I needed to delete the address and then re-enter it.

Every record created can be even further customized from a visual perspective. For databases with a large number of records, colors should make browsing much easier.



I didn't try it, but Data Guardian settings offer an option of database synchronization. This is probably related with the desktop version of the Data Guardian product, but as I am not using it I wasn't able to test it.

Overall Data Guardian is a rather good solution for storing various types of private data on your iPhone.

RSA Conference 2009

20 April-24 April 2009 - Moscone Center, San Francisco
www.rsaconference.com/2009/US/ (enter priority code: HN128)

InfoSec World 2009 Conference & Expo

7 March-13 March 2009 - Disney's Coronado Springs Resort, Orlando, FL
www.misti.com/infosecworld

Infosecurity Europe 2009

28 April - 30 April 2009 - Earls Court, London, UK
www.infosec.co.uk/helpnetevents

6th Annual CISO Executive Summit & Roundtable 2009

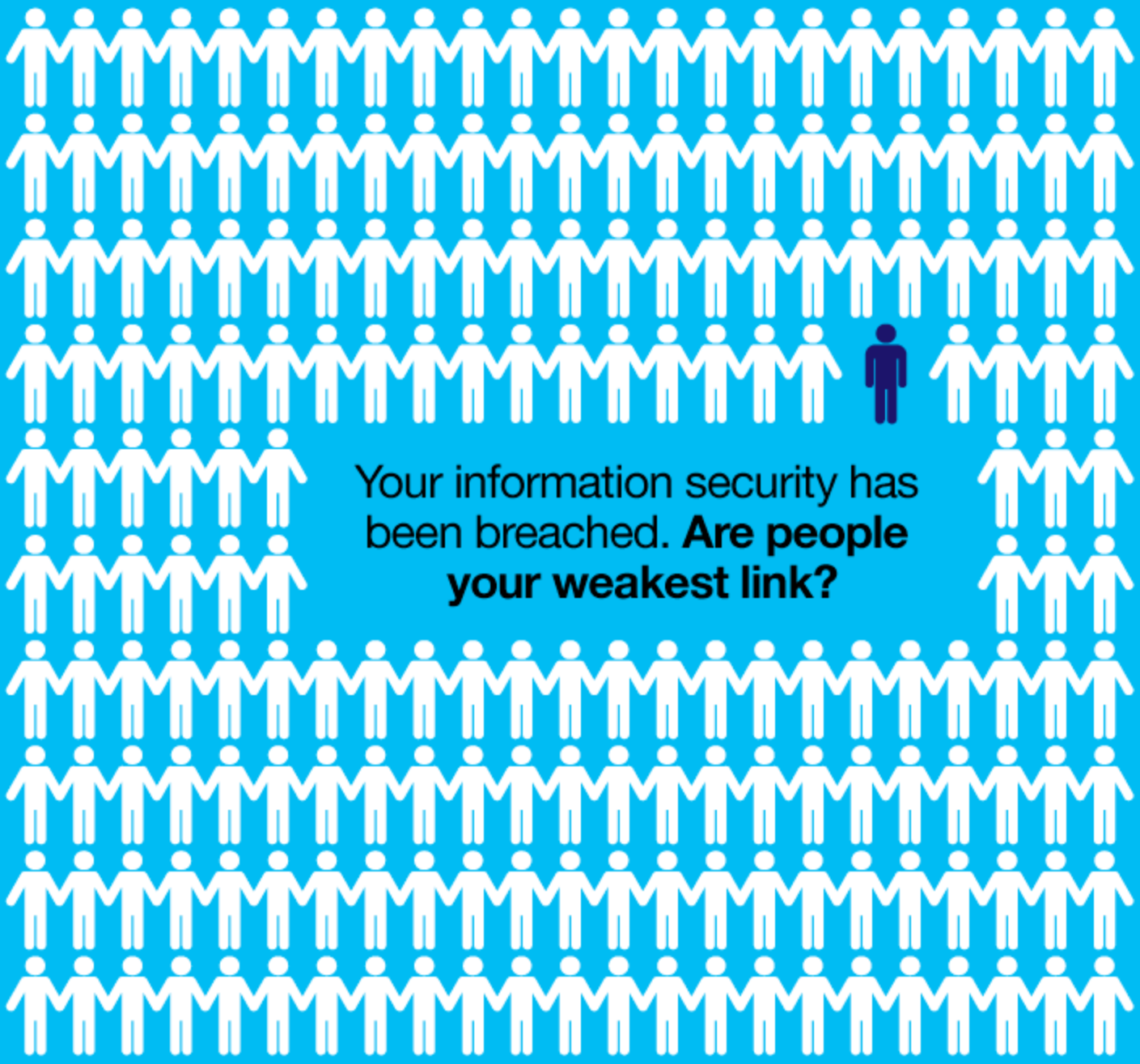
10 June-12 June 2009 - Marriot Hotel, Lisbon, Portugal
www.mistieurope.com/ciso

2009 USENIX Annual Technical Conference

14 June-19 June 2009 - Town & Country Resort and Convention Center, San Diego, CA
www.usenix.org/events/usenix09/

CONFidence 2009

15 May-16 May 2009 - Krakow, Poland
2009.confidence.org.pl



Your information security has been breached. **Are people your weakest link?**

Information Security - Combining effective technology and informed people.

Attend Infosecurity Europe 2009 and…

- Increase information security awareness amongst your employees and suppliers by attending the free education programme
- Meet over 300 of the top technology, service and solution suppliers in the industry

Visit Infosecurity Europe, Europe's No.1 information security event.

New venue for 2009!

28-30 April 2009
Earls Court
London | UK

Register for FREE ENTRY

at www.infosec.co.uk

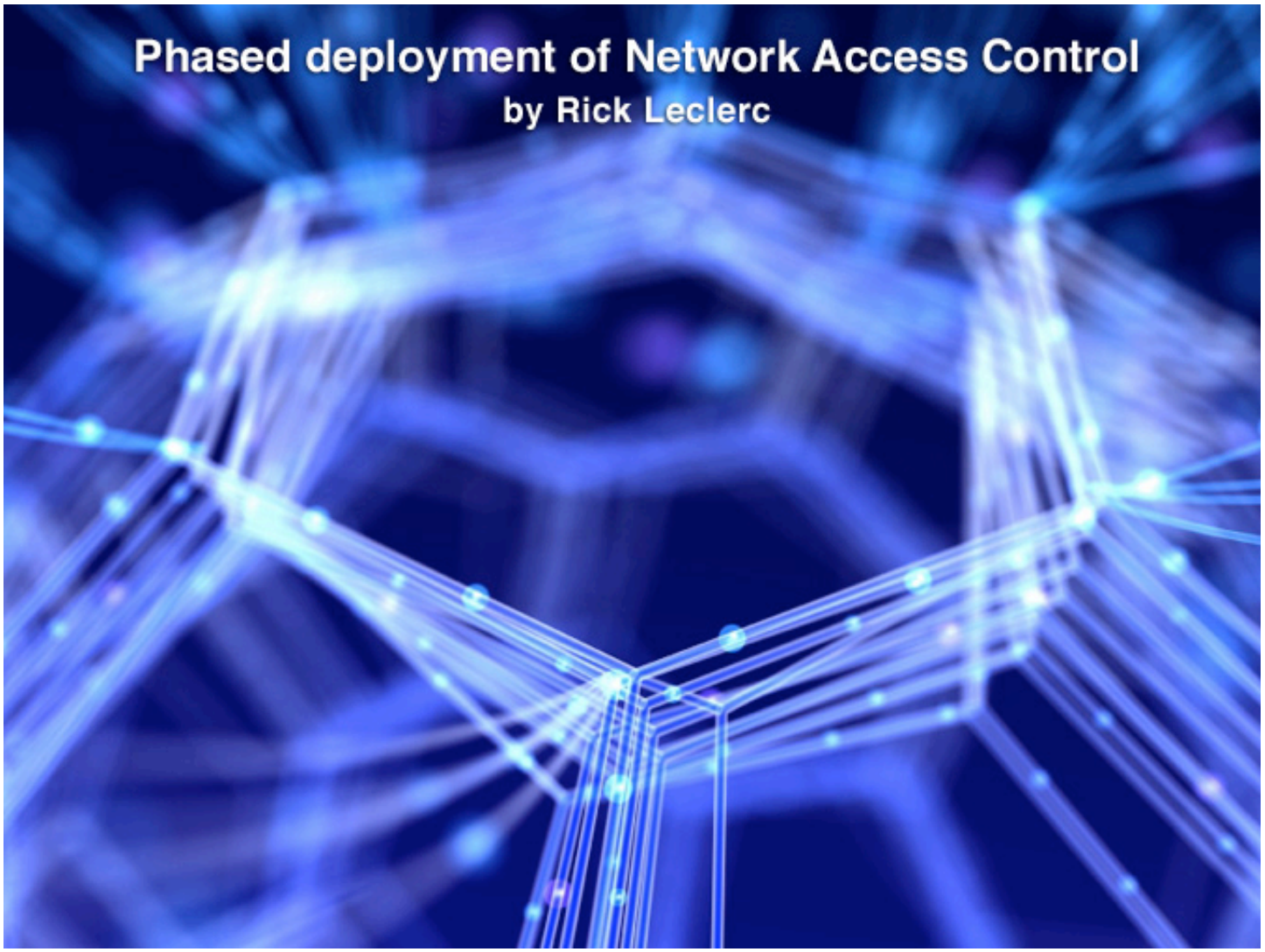
Reed Exhibitions®

infosecurity® EUROPE

*Visitors not registered by 5pm on Friday 24th April will be charged a £20 entrance fee.

Phased deployment of Network Access Control

by Rick Leclerc



Network Access Control (NAC) is an essential gatekeeper and a valuable defense mechanism for an organization's network. NAC provides information and controls on endpoints for network security, asset management, and regulatory compliance, making these processes more efficient and saving both time and money. While many organizations know NAC can improve security, they are uncertain of the best way to introduce it.

Out-of-band NAC architectures provide the greatest security and flexibility and are the least intrusive as well as the most scalable and cost-effective.

An out-of-band architecture is one that communicates with elements in the larger NAC system (host-based agents, AAA systems, network infrastructure such as wired and wireless switches, deep-packet inspection devices) outside of the data communication path to assess user and device posture and enforce usage policies. To enforce policy at the network edge effectively, a NAC system must be able to communicate with edge devices – wired, wireless, or VPN – without disrupting the flow of normal production traffic.

Since it leverages the network infrastructure (switches, wireless APs) as Policy Enforcement Points, out-of-band NAC solutions require significant knowledge about existing devices, endpoints, and users before the "Control" mechanisms that implement policy decisions can or should be activated. An "all-or-nothing" deployment approach may seem indicated but this aggressive approach can cause delays and complications because any comprehensive Network Access Control project requires the cooperation of three teams within an organization: networking, security, and desktop.

A process with a 7-step phased approach involves these three groups, improves NAC

deployments, reduces administrative burdens, and minimizes the impact on the network user.

Background

Many network and security teams, pressured to create a more secure environment, struggling to meet regulatory deadlines, or impatient for results, may try to implement control mechanisms too quickly. Typically, they encounter one or more of these common problems:

• Users are locked out of the network because authentication servers become isolated from the clients who are attempting to authenticate.
• No one can print because the printers have been inadvertently removed from the production network.
• No one can send or receive email because the email servers are isolated from the production network.
• System failures occur because HVAC systems and medical devices have been triggered to reboot due to NMAP scans.
• Clients are asked to upgrade their anti-virus definitions but they are isolated from the production network and lack access to the resources needed.

Colleges and universities have been early adopters of NAC due to their large student populations which use personally-owned computers to access academic networks. University IT staffs typically deploy NAC in the dormitories first because most universities are not concerned if the students can't connect to the school's production network. In this environment, security has a higher priority than usability and control mechanisms can be introduced immediately.

Enterprises, healthcare organizations, financial institutions, and government agencies with professional user populations are much less willing to introduce control early in a NAC deployment, however, for some very good reasons. When control is introduced too quickly and without proper preparation, deploying NAC can be risky.

• New technology projects usually have both an operational and a political time "window" during which they must complete initial trials and production deployments to be successful. If the project misses the window, the political impact can be significant.
• New technology projects typically impact multiple functional areas within an organization and success requires input and buy-in from all functions involved.

NAC is about letting the "good guys" on the network and fending off the "bad guys" while keeping the organization's wheels turning. The recommended best-practice approach to deploying a NAC solution to meet these seemingly contradictory goals involves a phased approach.

The following seven phases will allow organizations to increase value with each step while limiting the risk of negative impacts on the business applications and processes that run over the network. These phases involve three basic functions:

1. Monitoring the network, the devices, and the users for a period of time to identify who the "good guys" and the "bad guys" are as quickly as possible with minimal changes to the network and no changes to the user experience during network access.
2. Identifying the most vulnerable areas of the network to highlight immediate risks and pinpoint the best place(s) to start with policy-based enforcement and control.
3. Identifying the enforcement options available in each area of the network defines the available choices once it's time to implement them. Options include: DHCP, VLANs via 802.1x, VLANs via CLI, VLANs via Radius-MAC authentication, inline enforcement, and vendor-specific isolation mechanisms.

Phase 1 – Device and user monitoring

This phase answers the following questions:

1. "What types of devices are connecting on each area of the network?" This may include:

• Conference rooms
• Public WiFi
• R&D offices
• Sales bull pen
• Labs
• Classrooms

2. Who is authenticating each device, if anyone?
3. What area of the network poses the biggest security threat?
4. Does the network have switches that support the security features required to act as policy enforcement points?
5. Does the network have wireless access points or controllers that support the security features required to act as policy enforcements points?
6. Does the infrastructure have VPN concentrators that support the security features required to act as policy enforcement points?
7. What is the best enforcement mechanism for each section of the network?

Device and user monitoring includes:

• Identifying all the network switches, wireless access points, wireless controllers, and VPN concentrator devices to which end users will connect to obtain network access.
• Identifying all endpoints by MAC address, IP address, switch port, connect time, and disconnect time.
• Classifying, categorizing, and profiling each end point based on a set of defined rules.
• Identifying who is assigned to and accountable for each device.
Phase 1 starts with automatically discovering network switches and devices based on IP address, SNMP MIB-II system object ID, and system descriptor. The results, a complete list of switches, will help determine the enforcement options for the control phase. These switches will also collect additional endpoint identity information. Access-layer switches are read to obtain MAC address, switch port, connect time, and disconnect time.
Distribution/core layer switches are read to obtain IP address to MAC address mapping information. This simple collection and correlation of information starts creating an inventory and asset-management database.

The second part of Phase 1 involves Active Directory login scripts. Data sent from the login scripts allows the NAC server to associate 'username' and 'hostname' with the device information. MAC address and 'hostname' typically become permanently associated in the database, while MAC address and 'username' are a temporary association, lasting only for the duration of the user login.

This phase has two results: the identity of every end point with the associated user login and the identity of all endpoints without user logins.

Phase 2 – Endpoint compliance monitoring

This phase determines endpoint operating system patch levels, installed applications, anti-virus and anti-spyware definition levels for machines that can be automatically accessed by software agents pushed from Active Directory GPOs. It also identifies which machines meet the organizational requirements, and which machines require user interaction to install and activate a persistent endpoint compliance agent.

Leveraging Active Directory Group Policy, Alteris or another automated "software pushing" mechanisms, an agent will examine the connecting machine (windows registry, files, etc) and return the results to the NAC server.

Active Directory groups define "roles" within the NAC database. This role assignment determines which policy checks the agent performs and also determines the scheduled timing of any revalidation checks done by the NAC server. In addition to revalidation checks initiated by the NAC server, a role-based policy can be defined to "monitor" specific components between revalidation checks. All of these checks are performed transparently to the end user with no impact to productivity. All results are saved within the NAC server database and are available for viewing through the administrative GUI and through reports.

Phase 3 – Behavior and signature-based violations

This phase identifies the users and devices responsible for post-connect policy violations. It answers the question, "What device is misbehaving and where is it?" and requires integration between the NAC system and deep packet inspection systems.

Inline signature and behavior-based monitoring systems send SNMP traps and/or syslog messages to the NAC server. The NAC server obtains the IP address of the offending device, associates this IP address with the

corresponding MAC address, hostname, and username, and stores this association in the NAC database.

Phase 4 – Notification of end users and administrators

The logical next step in a full NAC implementation is to notify network administrators of the results of each of the previous three monitoring-only phases. These notifications give the network administrator the information necessary to effectively implement the control portions of the NAC deployment. As end users are notified of policy violations they become aware of the new NAC system and start changing their behavior to comply with the new access control policies.

Notification options to end users could include: (1) email from a predefined email account and email server triggered by the NAC server, (2) a messaging option using the persistent agent, or (3) an SMS message triggered by the NAC server. Administrators can be notified by email and SMS messages from the NAC server to a group of administrators. The NAC server can also notify other management systems of important events through a 'north-bound' SNMP or syslog interface.

Phase 5 – Identity-based control: network isolation for unknown machines

With the organization-owned machines already identified in the database, there is minimal risk in activating this identity-based control because all known machines will still be able to access the production network. Identity-based control includes the following:

• Isolation of unknown machines using the method chosen for each area of the network
• Web-based captive portal for authentication/registration of the unknown machine
• Role-based production network access for the newly registered machine

Phase 6 – Compliance failure-based control: quarantine and self remediation

In many NAC initiatives, blocking non-compliant machines from the production network is the primary goal. These machines pose the most risk to the environment and could potentially propagate serious worms and/or viruses around the network. Preparing for this step probably needs the most work from the network team because it requires a self-remediation function to make the NAC initiative as effective as possible. Quarantining non-compliant machines cannot trigger more help desk calls and create more work than it prevents. It is imperative that users are prepared for this step in the NAC deployment so communicating to the user population is a key step to success.

Once quarantining has been activated, users can either be directed to contact the helpdesk, fix their machines themselves, or wait for an automated patching system to update their machine. It is up to them which option to choose. As long as the network is configured to support self-remediation, this option should produce the least amount of work for the help desk. Once the users have followed the directions to update their machines, they can initiate the agent again and validate the machine is now up-to-date. When the NAC server realizes the machine is compliant, the machine will be moved out of isolation and onto the production network.

Phase 7 – Post-connect behavior-based control: disabling or quarantining clients

Isolating users based on post-connect events poses the same concerns as isolating users based on compliance failures. The difference between phase 6 and phase 7 is that phase 6 usually isolates users before they connect while phase 7 takes users off the production network and moves them to an isolation network.

If the user is doing something important to the business, disrupting that effort due to a behavior violation had better be for a good reason. The monitoring and notification phases of post connect behavior-based control are critical to minimizing the number of false positives. The network administrator must choose from several actions that can be taken against the offending user/device based on the amount and the level of information obtained from the inline device. These actions include disabling the switch port, disabling the host MAC address, or quarantining the host MAC address.

Completely blocking access for the offending user eliminates the risk to the network, but it may not be the most effective action. Blocking the offending user via quarantine VLAN eliminates the risk to the production network while notifying the end user why he was removed from the production network. The user may even be notified exactly why he was isolated and receive specific instructions on how to address the problem and return to the production network. This last scenario requires the most setup and configuration prior to activation, but it also accomplishes three major priorities for any organization:

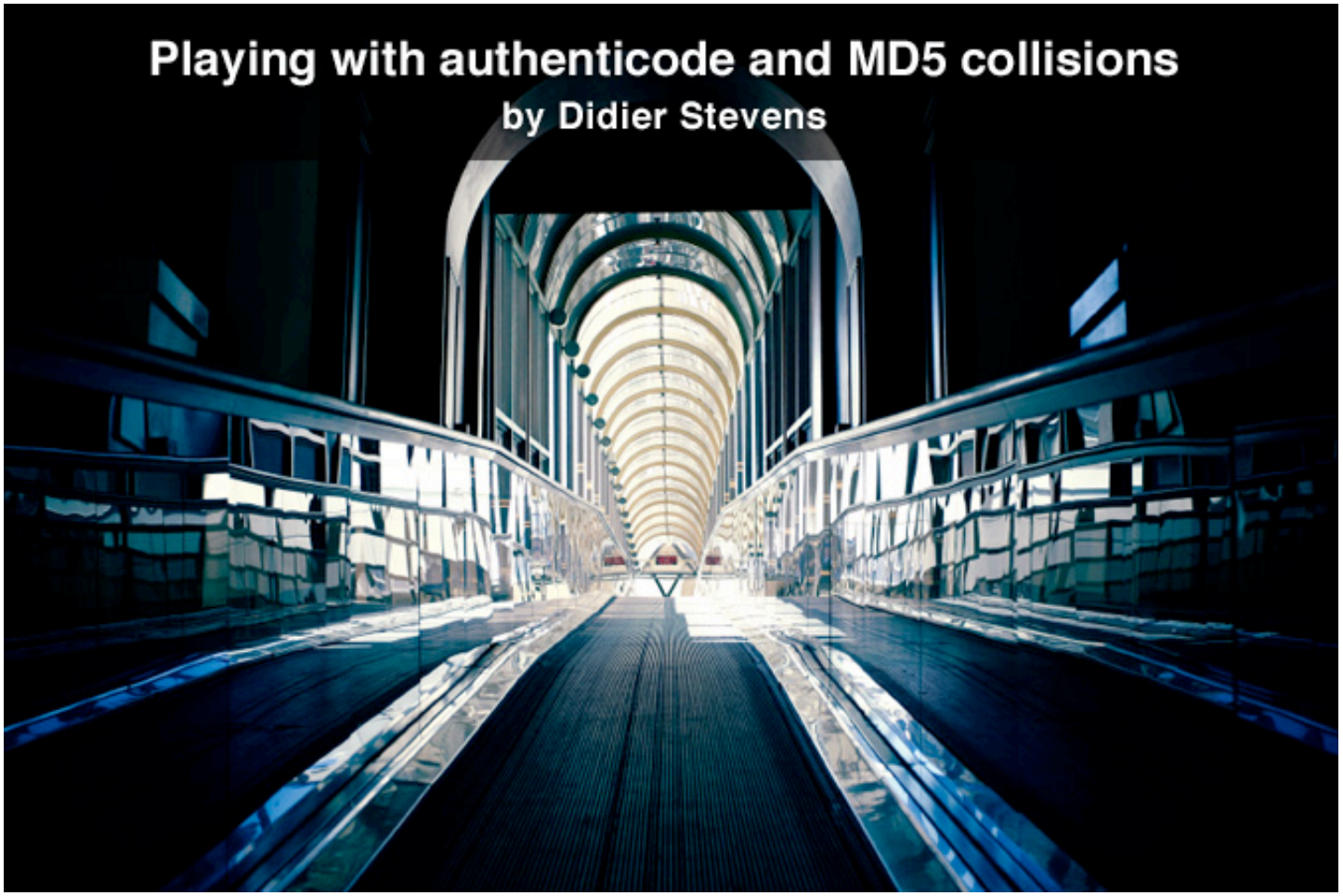
1. It keeps the production network free from misbehaving users/devices
2. It allows misbehaving users/devices to "fix themselves" and return to the production network
3. It minimizes the number of calls to the help desk.

Summary

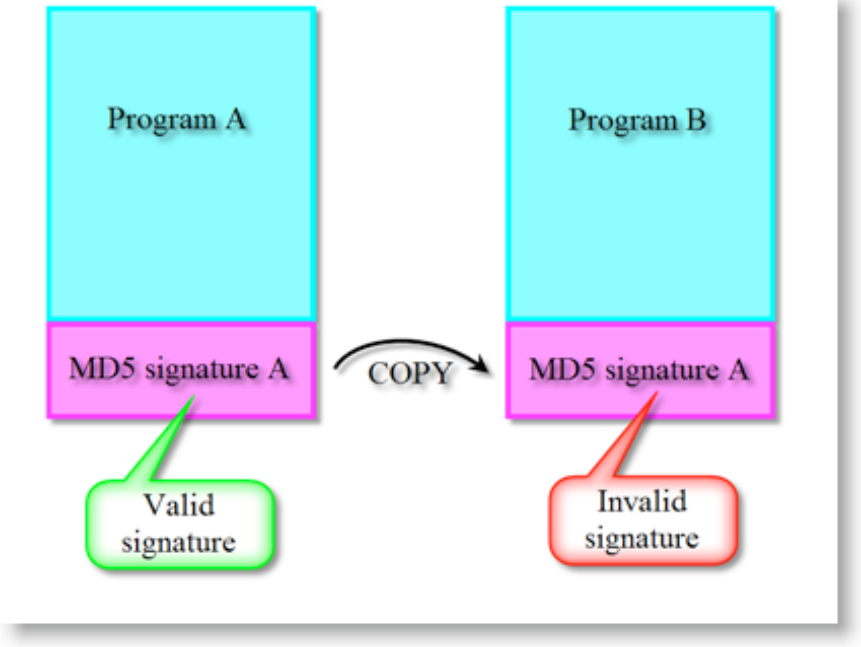
By adopting a phased approach to NAC deployments, organizations establish a predictable path and timeline to understand and implement this powerful new technology.

Seven distinct phases are involved in a full NAC implementation, with each building on the results of the previous phase to gradually discover all network infrastructure elements, users and devices, define and validate access and usage policies and determine the most effective policy enforcement and control mechanisms available in the existing infrastructure.

Rick Leclerc is the VP Technology Partnerships at Bradford Networks (www.bradfordnetworks.com). Rick is responsible for establishing technology partnerships within the security and networking industry. He is a senior networking industry veteran with an extensive background in customer relations, business partner development and the dynamic security market. Rick's professional background includes 10 years as a Senior Director for Product Development at Aprisma Management Technologies.



Back when I researched Microsoft's code signing mechanism (Authenticode), I noticed it still supported MD5, but that the signtool uses SHA1 by default. You can extract the signature from one program and inject it in another, but that signature will not be valid for the second program. The cryptographic hash of the parts of the program signed by Authenticode is different for both programs, so the signature is invalid. By default, Microsoft's code signing uses SHA1 to hash the program. And that's too difficult to find a collision for. But Authenticode also supports MD5, and generating collisions for MD5 has become feasible under the right circumstances.

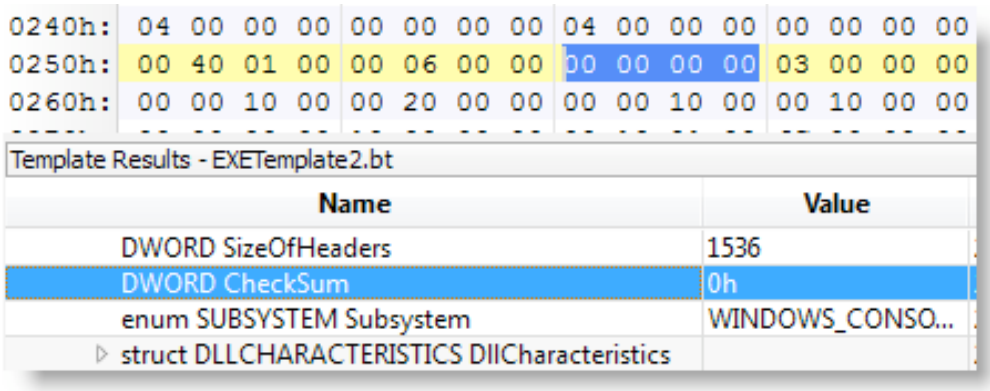


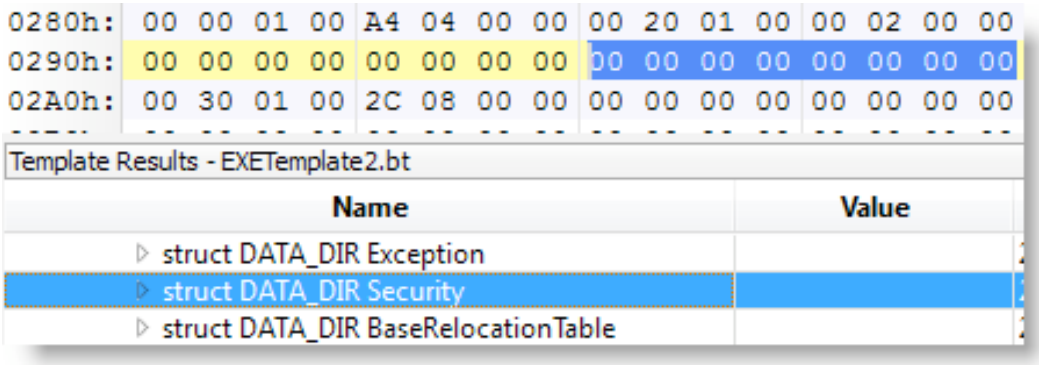
If both programs have the same MD5 Authenticode hash, the signature can be copied from program A to program B and it will remain valid. Here is the procedure I followed to achieve this.

I start to work with the goodevil program used on this MD5 Collision site (tinyurl.com/35ypsn). Goodevil is a schizophrenic program. It contains both good and evil in it, and it decides to execute the good part or the evil part depending on some data it caries. This data is different for both programs, and also makes that both programs have the same MD5 hash.

The MD5 collision procedure explained on Peter Selinger's page will generate 2 different programs, good and evil, with the same MD5 hash. But this is not what I need. I need two different programs that generate the same MD5 hash for the byte sequences taken into account by the Authenticode signature. For a simple PE file, the PE Checksum (4 bytes) and the pointer to the digital signature (8 bytes) are not taken into account (complete details at tinyurl.com/d2kxd). That shouldn't be a surprise, because signing a PE file changes these values.

So let's remove these bytes from PE file goodevil.exe, and call it goodevil.exe.stripped. The hash for goodevil.exe.stripped is the same as the Authenticode hash for goodevil.exe.



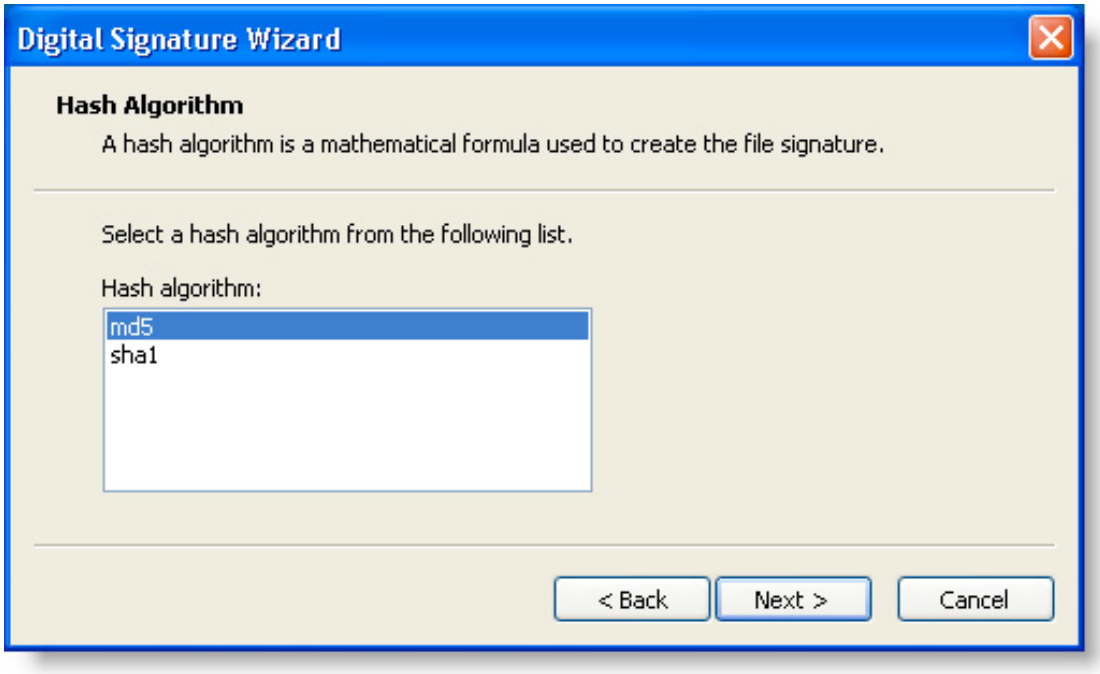


Now I can compute an MD5 collision for goodevil.exe.stripped, as explained on Peter Selinger's page. (I could also have modified the MD5 collision programs to skip these fields, but because this is just a one shot demo, I decided not to).

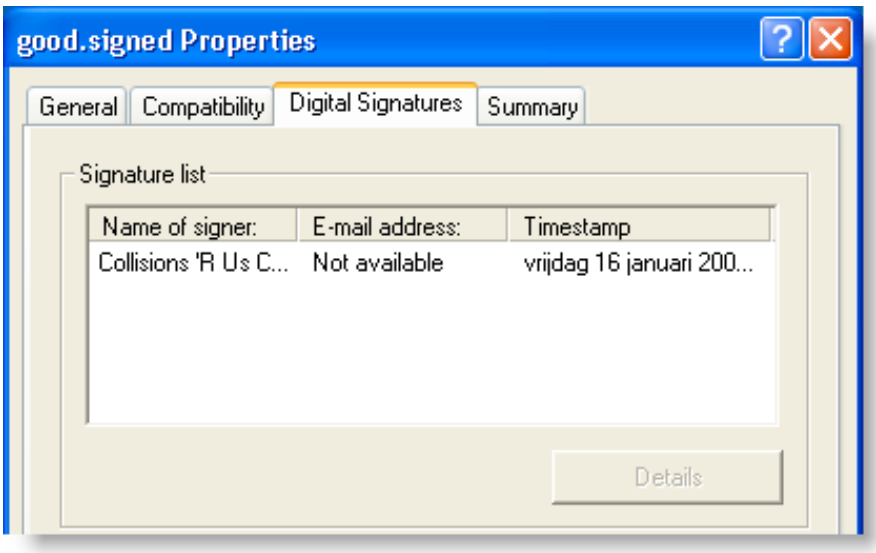
After about an hour, I have 2 new files, good.exe.stripped and evil.exe.stripped, both with the same MD5 hash. I transform them back to standard-compliant PE files by adding the checksum and pointer bytes I removed (giving me good.exe and evil.exe). Now the MD5 hashes are different again, but not the Authenticode MD5 hashes (Authenticode disregards the PE checksum and the signature pointer when calculating the hash).

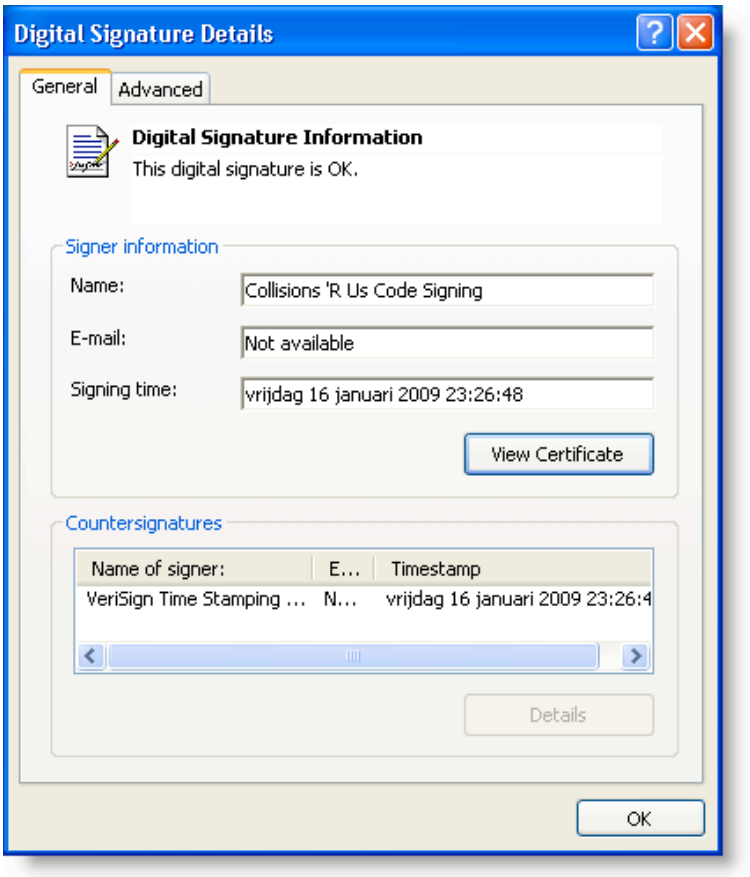
Now I sign good.exe with my own certificate and I select custom signing:

This allows me to select MD5 hashing in stead of the default SHA1:

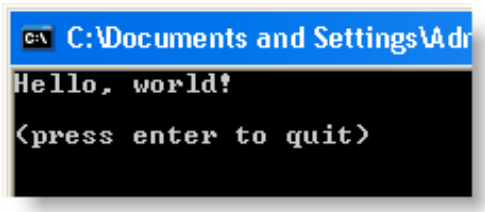


Now good.signed.exe is signed:



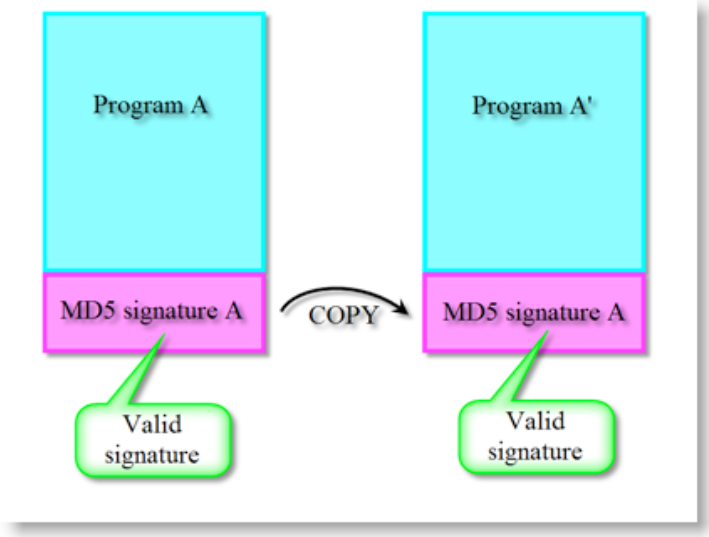


The signature is valid, and of course, the program still works:

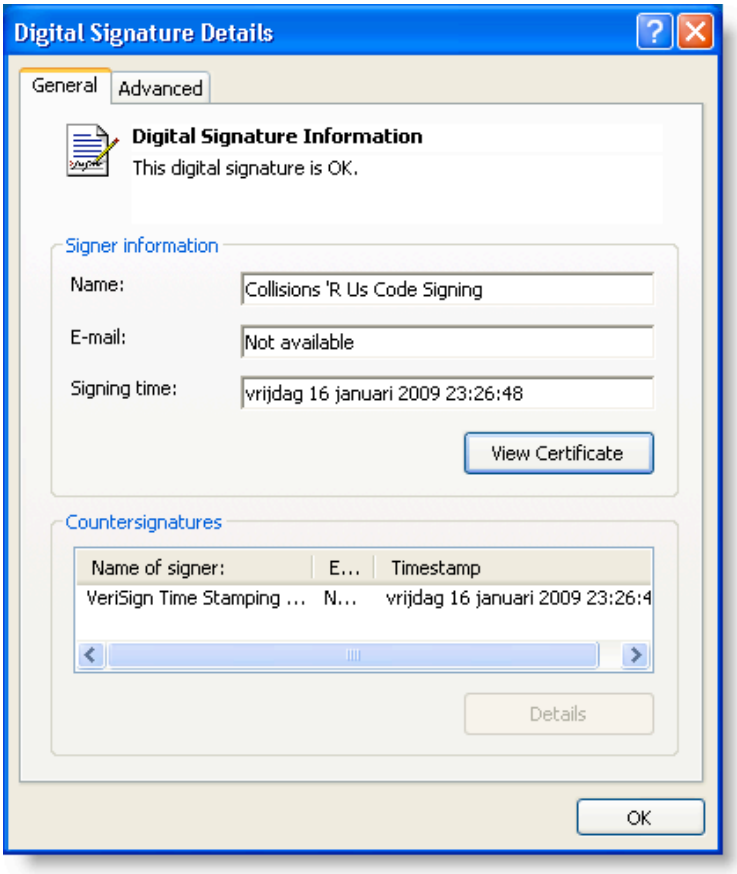


Let's summarize what we have. Two programs with different behavior (good.exe and evil.exe), both with the same MD5 Authenticode hash, one with a valid Authenticode signature (good.signed.exe), the other without signature. Now I extract the signature of good.signed.exe and add it to evil.exe, saving it with the name evil.signed.exe. I use my digital signature tool disitool (tinyurl.com/5h74zx) for this:

disitool.py copy good.signed.exe evil.exe evil.signed.exe



This transfers the signature from program good.signed.exe (A) to evil.signed.exe (A'). Under normal circumstances, the signature transferred to the second program will be invalid because the second program is different and has a different hash. But this is an exceptional situation, both programs have the same Authenticode hash. Hence the signature for program evil.signed.exe (A') is also valid:

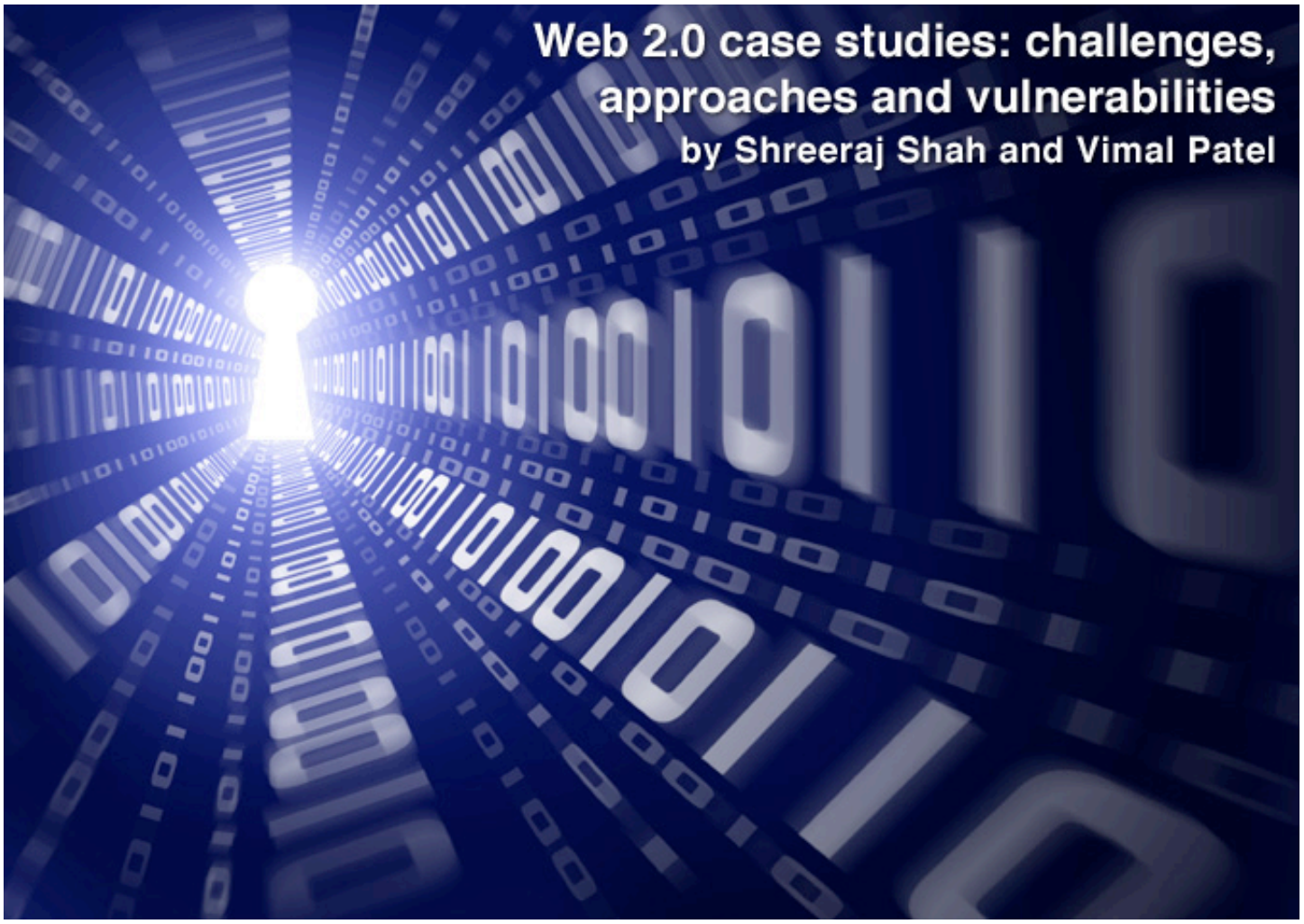


evil.signed.exe executes without problem, but does something else than good.signed.exe:

This demonstrates that MD5 is also broken for Authenticode code signing, and that you shouldn't use it. But that's not a real problem, because Authenticode uses SHA1 by default (I had to use the signtool in wizard mode and explicitly select MD5 hashing). In command-line mode (for batching or makefiles), the signtool provides no option to select the hashing algorithm, it's always SHA1. And yes, SHA1 is also showing some cracks (tinyurl.com/4rl78), but for Authenticode, you have no other choice.

You can download the demo programs and code signing cert at this location - tinyurl.com/bogldn.

Didier Stevens (CISSP, GSSP-C, MCSD .NET, MCSE/Security, RHCT) is an IT Security Consultant currently working at a large Belgian financial corporation. He is employed by Contraste Europe NV, an IT Consulting Services company (www.contraste.com). You can find open source security tools on his IT security related blog at DidierStevens.com.



Web 2.0 case studies: challenges, approaches and vulnerabilities

by Shreeraj Shah and Vimal Patel

Web applications are a continuously evolving phenomenon. Over all these years, we witnessed the introduction of new ways of designing and building web applications. New architectures are evolving and industrial strength applications are emerging. From the beginning of 2006, we saw the coming of a new range of applications in the field – the so-called Web 2.0 applications. Applications that (from a security perspective) need some twisting and tweaking of methodologies when it comes to assessment.

Web 2.0 applications are emerging at a rapid pace and also penetrating deeper into the corporate structure as Enterprise 2.0 applications. Adaptations of Ajax, Flex, SOA, RSS Feeds, JSON structures, etc. are used continuously across applications. Old applications are getting a new look through these technologies and platforms, while fresh applications are written using only these building blocks.

By the end of 2008 we have seen and assessed a good amount of applications that are now well molded into a Web 2.0 framework. A Web 2.0 application adaptation is not restricted to one industry segment but applicable to all verticals like financing, insurance, portals, etc. If the Internet is the network of networks then Web 2.0 can be perceived as the application of applications.

Cases and challenges

We came across a set of applications during the work and different Web 2.0 components were implemented in them. Components like widgets, blogs, RSS feed readers are becoming an integral part of an application. During 2008, we faced several new cases and challenges while performing Web 2.0 application assessment and audits. There were some interesting vulnerabilities and mechanism to discover. Application profiling and crawling is a very difficult task to perform when an entire site is driven by JavaScript or Flash/Flex.

Traditional crawling and discovery by HREFs failed in several cases. To do some blackbox crawling we needed to deploy “in browsing” crawling strategies and techniques where enumeration was done in the context of DOM and within its event model. There is no place for typical crawling in Web 2.0 assessments, and crawling needs to be event driven. On several applications just 4-5 links were discovered by crawlers, while event driven crawling along with JavaScript parsing was able to discover 100+ resources buried in the application’s client side layer.

In some cases resources are easy to identify by crawling, but without DOM and its context it is not possible to fuzz. Traditional fuzzing is of no use when we just carry out activities on name value pairs. Now, it is imperative to fuzz JSON, XML or Object streams because these streams can carry payload for exploitable vulnerabilities. Also, these structures are well crafted using SOAP or JSON. If a structure is malformed during fuzzing, then the actual vulnerability will not get discovered but the error message that comes back is of different type and not indicating vulnerability. For example, if SOAP is malformed then you get a SOAP context error and not an SQL interface error. Hence, it is imperative to fuzz the parameter and not disturb the envelope or structure.

DOM based XSS tracing is another important challenge. You have to trace a variable in the JavaScript and its potential source. It is easier to find this vulnerability by using source code scanning over the typical blackbox approach. Also, asynchronous activities are very common in Web 2.0 applications - we inject something in one area and an event takes place after a time on a completely separate part of the application.

Web 2.0 application entry points are not just HTTP parameters; applications are running in mashup and making several API calls across different application domains. This makes the entry point identification a challenging task. Once again, it was difficult to analyze it with just blackbox, one needs to take a peek at the source code and during our analysis we were able to unearth several new vulnerabilities using source analysis.

Authentication mechanisms are different with Web 2.0 applications and it is imperative to test them with Single Sign On and SAML in cases where the application is running on a multi-domain framework. Doing the assessment without its support over HTTP is of no value since requests haven’t the right context in place.

Applications are running with some interesting authorization mechanisms where tokens are embedded in JSON or XML structures and they are implemented in the client side JavaScript. This authorization checks are easy to bypass after analyzing the client side code.

Business logic used to reside on server side in traditional applications but with Web 2.0 application it is not the case. Applications are getting written at both the end and part of logic gets implemented in Ajax code residing on client side or in flash component in some cases. This shift is happening to make application much faster and making it more user friendly as well but it is giving an opportunity for attacker to analyze the code. Now it is imperative to do a full assessment of the business logic analysis with the help of source code both at server and client end to discover business logic flaws. In some cases business logic flaws were identified on the client side and they were easy to manipulate and tamper with. Business logic tampering and exploitation were possible with Web 2.0 applications running with JSON and XML as their primary communication drivers.

Blog application plug-ins to the application is a major source of XSS with Web 2.0 applications. It can be discovered by traditional analysis on name value pairs but uncovering of these resources was tricky since calls were going over Ajax and were missed by traditional crawling.

A Cross Domain Bypass can be executed by two methods. Either by putting proxy code on the domain or by building callback wrapping for JavaScript. In a few cases, the proxy code was not sanitizing the content coming from different sources and it was possible to inject JavaScript snippets and other malicious code through it. We discovered that by analyzing the source of the proxy implementation.

Callback wrapping was implemented by a few applications and, in those cases, by analyzing JavaScript we discovered that eval() calls were the culprit for potential XSS. Callback wrapping puts your end client at the mercy of some other domain while application is running within your domain's context. Lots of clients' side controls are required before implementing it. In some cases it was very critical to discover these callbacks in a large source base and then tracing them across.

SOA analysis and relevant component reverse engineering (from footprinting to the actual assessment) were done and tools were created and used for the assessment. Proxy code is needed for SOAP building to inject and test the implementation.

Addressing challenges with tools and approaches

To address the above challenges and problems, the following tools and approaches were developed for application assessments.

- It is important to have context sensitive, DOM-based crawling technology and a technique to address the asset discovery problem. We built a dynamic DOM crawler engine to do advanced crawling when an event had to be analyzed and if it was pointing to an XMLHttpRequest call then we needed to trigger it to discover hidden resources.
- Fuzzing and simulation techniques are added to address other streams that are not traditional name-value pairs but capable of addressing JSON or XML.
- JavaScript parsing and a source code analyzer are required to identify potential DOM based vulnerabilities and entry points. We implemented a small JavaScript analysis engine to discover a set of vulnerabilities.
- Overall, source code analysis proved much more effective than the typical blackbox scanning approach. It was impossible to identify certain entry points with scanning and we were able to discover them from the source code.

The above approaches, along with the traditional methodologies helped us to discover potential vulnerabilities in the set of applications we reviewed.

A different and interesting set of Web 2.0 type vulnerabilities and cases

Cross widget injections
Applications are implementing widgets and gadgets into application pages and in cases where widgets are running in the same DOM. This opens up a cross widget injection and content loading in one – a widget can both read and modify the content of another widget. This also opens up a set of different attack vectors for an attacker. It is important to have segregated DOM using iframe or any other way to avoid this breach.

SQL injection with XML/JSON
SQL injections going over JSON or SOAP streams are common. If we analyze the typical error messages coming back from Web 2.0 resources or assets, responses are not 500 HTTP errors but exceptions residing in JSON streams or SOAP envelopes and in some cases message code is 200 OK. One needs a combination of advanced fuzzing and error message interpretation capabilities to discover these vulnerabilities. We found a common issue with Web 2.0 applications and it is easier to exploit it like traditional SQL injections.

Asynchronous injections
In some cases the application is doing asynchronous operations. The application is taking dates from the end user and generating respective orders details in RSS format offline against databases and tables. The code for offline process may be triggering at 12 o' clock midnight. This is an SQL injection point and from source code analysis it is obvious that no validation was done and it is vulnerable to SQL injection in asynchronous fashion. It is interesting to analyze all the possible asynchronous functionalities implemented in Web 2.0 applications.

One click injection with RSS feed readers
In an RSS feed reader the end user can configure the feeds. With applications that support cross-domain proxy and do not have the proper validations on proxy code, it is simple to inject JavaScript code into the malicious RSS stream. This stream reloads the DOM and the malicious links waiting for execution when the HREFs get clicked on by the user.

This leads to a click injection into an application with a target domain. It is possible to steal cookies or execute code in the end user's browser if script gets executed with the current DOM context.

LDAP bypass through SOAP
In some cases SOAP is integrated into the LDAP authentication mechanism either through the header or a part of the body. It is possible to perform a LDAP injection attack and retrieve internal information from the back end server. This is an interesting vulnerability to explore when SOAP is authenticating, the authorization mechanism is implemented and this implementation is weak and exploitable.

Cross Site Request Forgery with JSON/ XML
CSRF is possible with Web 2.0 applications when the client is sending JSOM or XML streams to the application pages. It is feasible to craft a POST request that can hit the application from the browser without the end user's consent. In the applications there are several pages where CSRF checks were not in place and a successful exploitation was possible. In some cases SOAP requests can be crafted as well. It is imperative to check the content-type to segregate Ajax calls from the traditional form based POST requests. It is an old attack in a new style.

XPATH injections for authentication bypass
Applications can call back-end over XML pipe and authentication credentials can be compared using XPATH. In this case it is feasible to bypass authentication and get access to the system. XML and JSON are becoming very popular structures for data processing and usage of XPATH can be abused in Web 2.0 applications. This attack vector can be detected with source code analysis much more easily then by scanning with zero knowledge.

XSS and mashup exploitation
Untrustworthy sources of information are one of the major issues for Web 2.0 applications. Applications are exploiting various sources of information in the form of a mashup. We were able to identify a few locations where exploitation is possible either by feed or by API call across applications. Once again, cross-domain by-pass implemented by developer either by having proxy at server end or supporting a callback was a major issue, as well as no validation on the incoming content.

Authorization and data access from JavaScript
Web 2.0 applications are doing certain things differently by having tokens in JSON or XML and few applications where JavaScript has authorization logic and tokens can be manipulated. These tokens can be manipulated and tampered with to gain unauthorized access to the application. Also, in the few cases we have seen, data queries are going directly to the data access layer over Ajax calls and that can be exploited for potential SQL injections.

Conclusion
Web 2.0 applications are changing the rules of assessment and hacking. We see traditional approaches and methodologies failing in addressing several new issues and an automated approach is not helping in the search for vulnerabilities. On the blackbox side, manual review along with techniques and tools is essential. To some extent, whitebox testing is a great way to determine the range of new vulnerabilities with Web 2.0 applications that may get missed by blackbox testing. Assessment and testing are becoming increasingly more interesting and challenging in the Web 2.0 era. New challenges are bringing new ways and methods of hacking or defending. It is important to stay on the learning curve and spread knowledge in the corporate world to protect the next generation of applications.

Shreeraj Shah is the founder and director of Blueinfy, a company that provides application security services. He also worked with Net Square, Foundstone (McAfee), Chase Manhattan Bank and IBM in security space. He is the author of several security books, advisories, tools and whitepapers. He presented at numerous conferences and you can contact him at shreeraj@blueinfy.com.

Vimal Patel is the founder of Blueinfy where he leads research and product development efforts. Prior to founding Blueinfy, he held position of Vice President at Citigroup where he led architecture, design and development of various financial applications. Vimal's experience ranges from design of complex digital circuits and microcontroller based products to enterprise applications. You can contact him at vimal@blueinfy.com.

EUROPE'S PREMIER EVENT FOR INFORMATION SECURITY DIRECTORS

6TH ANNUAL

CISO EXECUTIVE SUMMIT & ROUNDTABLE 2009

MIS TRAINING INSTITUTE

DELIVERING PRAGMATIC & VALUE-ADDING SECURITY: REALISTIC SECURITY FOR BUSINESS REALITIES

MARRIOTT HOTEL LISBON 10–12 JUNE 2009

HEAR MOTIVATING & CANDID SUCCESS STORIES FROM INFORMATION SECURITY PRACTITIONERS & GURUS FROM THE FOLLOWING COMPANIES:

- Microsoft Ltd (UK)
- Deutsche Bank
- DHL
- Lloyd's
- BT
- Dresdner Kleinwort
- Novartis Pharma AG
- DU Telecom
- Webster University (Geneva)
- BT Counterpane
- Saladin Technical Services plc
- BurrillGreen Ltd
- ITSEC Associates Ltd
- DVLA - provisional

REGISTER NOW:

Online: WWW.MISTIEUROPE.COM/INSECURE **TEL:** +44 (0)20 7779 8217 **@:** AMCPARTLAN@MISTIEUROPE.COM

JOIN PEERS & BE INSPIRED! TOP REASONS TO JUSTIFY YOUR ATTENDANCE AT THIS YEARS' SUMMIT

- Hear how other organisations are ensuring that their security strategy remains focused, uncompromised and integral to the business: Managing threats day to day and preparing for the future
- Be assured you aren't missing any tricks on how to manage information security through periods of extensive change and development
- ROI to deliver information security projects: Linking with internal and external customers; Building teams that return money to business lines
- Unique learning via case studies, high profile keynotes, panel debates and roundtables will probe the CISO role and realities
- The CISO Roundtable is the unrivalled benchmarking forum for open debate into security's hottest challenges of the day with thought leaders. Includes a NEW closed session where you can safely share solutions on existing security incidents
- Build trust based relationships with your security peers! Expand your global security network with professionals who face the same set of challenges as you at Europe's premier event for CISOs

"Definitely worth the money within the first half day"

IT Security Officer, European Court of Auditors – Luxembourg at the CISO Summit 2008, Budapest

Silver Sponsor Seagate | Cocktail Sponsor BT | Gigabite Sponsor Aveksa | Association Partners (ISC)² ASIS INTERNATIONAL ISACA Belgium Chapter ISSA JERICHO ISF

Q&A: Jason King, CEO of Lavasoft

by Mirko Zorz

Jason King is CEO of Lavasoft. Founded in 1999, Lavasoft is "the original anti-spyware company", with over 350 million downloads worldwide for the flagship Ad-Aware product.

Do you think the average user is reasonably aware of Internet threats these days? Based on your experience, how does security awareness compare to a few years ago?

Security awareness among the average home computer user has improved markedly in the past years. Many users today know that anti-virus, anti-spyware, and a firewall are key in reducing their chances of becoming a victim of cyber crime.

Still, anyone with an Internet connection is in danger of falling prey to malware. Statistics tell us that as many as 90 percent of home computers have been infected with spyware. On top of that, industry studies show that over three-quarters of users lack core protection to keep their computers and private information safe. These figures make it clear that we must continue to be vigilant and get the word out to all users about security awareness.

While having security software in place is an essential step to keeping secure online, ultimately, consumers must also be knowledgeable about the threats they face as they navigate the Web. To stay a step ahead of malware that continues to both develop and circulate, computer users need to have an understanding of the current threat landscape and emerging trends. That's why, at Lavasoft, we strive not only to develop innovative products, but to educate users about online security – through our research and company blogs, monthly online security newsletter, and support forums.

What dangerous trends do you see in the world of malware creation?

From our vantage point, as the original anti-spyware protection company, we have witnessed quite a change over the past decade. In the past, hacking used to be seen as a means of wreaking online havoc for fun or

or fame. Today, malware authors have graduated from "cyber vandals" to "cyber criminals." Cyber crime continues to grow more organized, professional and targeted than ever before. As malware creators earn increasing profits, they turn around and release more sophisticated trojans, botnets and socially engineered attacks.

Since the malware landscape is profit-driven, cybercriminals' business and software development models mature to maximize a return of investment. As time goes on, this level of sophistication will drive innovation and competition among competing "malware businesses". As the levels of sophistication increase, the malware landscape will become increasingly intractable. With that said, the anti-malware industry will also continue to innovate to combat these threats. Another plus for consumers is that, as these criminal organizations proliferate, they are likely to become more visible and attract attention from law enforcement agencies.

In terms of specific threats users are faced with today, social engineering scams continue to thrive, attempting to scam users through fake websites, e-mail, and social networking sites. We've also seen a dramatic rise in rogue security products. Rogue security software is an application that appears to be beneficial from a security perspective but provides little or no security, generates erroneous alerts, or attempts to lure users into participating in fraudulent transactions. The number of rogue security and anti-malware software, also commonly referred to as "scareware," found online is rising at ever-increasing rates, blurring the lines between legitimate software and applications that put consumers in harm's way.

SINCE THE MALWARE LANDSCAPE IS PROFIT-DRIVEN, CYBERCRIMINALS' BUSINESS AND SOFTWARE DEVELOPMENT MODELS MATURE TO MAXIMIZE A RETURN OF INVESTMENT

With the threat landscape changing rapidly, how demanding is it to constantly improve a product such as Ad-Aware?

There is no debating the fact that the threat landscape is changing rapidly. By all counts, the amount of malware online grows exponentially on a daily basis. In this year's run-up to the holiday season, Lavasoft researchers saw a 462 percent increase in the amount of malware detected and added to Ad-Aware's threat database, compared to the same period last year.

Cyber criminals are relentlessly upping their tactics to get past the defenses of everyday computer users. That's why, at Lavasoft, we do have to work even harder to offer new features and technology to better protect the privacy and security of our customers.

A key example is our newly released Ad-Aware Anniversary Edition. With this new version of Ad-Aware, we focused our efforts on our core competence for online security – blocking, detection, removal, and clean-up – and we have poured our technological advances into these core areas. The result is a powerful, efficient product that offers improvements such as radically reduced computer resource use, rapid scan times, behavior-based heuristics methodology, overhauled real-time blocking, and much more.

How do you gather the intelligence needed in order to develop your software so that it can keep up with the bad guys?

At Lavasoft, we have a dedicated group of in-house security analysts who are focused on finding, analyzing, and categorizing malware, in order to make sure our software is able to find, detect, and remove the most current threats. In addition to that, we have a number of information-sharing partnerships with industry peers and groups. Despite the fact everyone involved belongs to different organizations, the mindset is that, by collaborating, we can each work to better protect today's computer users.

We also rely on direct submissions from our international network of malware-fighting volunteers (experts, enthusiasts, and everyday computer users). This includes our partnership through Lavasoft ThreatWork – an alliance of global anti-malware security volunteers actively fighting online threats.

Through the ThreatWork feature in Ad-Aware, users can easily and quickly submit suspicious files to Lavasoft researchers for analysis.

In terms of keeping up with the bad guys, in our new Plus and Pro versions of Ad-Aware, we also have included advanced behavior-based technology in order to pinpoint the very newest forms of malware. That means that Ad-Aware not only roots out and detects today's most prevalent threats with an extensive database of over 2 million threats, but it also protects against those not yet identified in our signature database.

What do you see your clients most worried about?

Not only do viruses and spyware remain chief online concerns, but the ultimate outcome of loss of private information – identity theft – is a very real and rising worry for many computer users. Consumers tend to be worried most about malware that grants unauthorized access to their bank accounts, compromises their privacy or leaves them vulnerable to ID theft.

Another concern we have identified among our consumers is having security products that deliver the absolute best protection without the usual drain on computer resources, or the extra bells and whistles that complicate other programs. Addressing that concern was a chief focus for our latest Ad-Aware release – in order to deliver advanced threat protection, in an easy-to-use and efficient product.

A great concern for our corporate clients is securing company data and protecting sensitive customer details that are stored on computers or passed back and forth electronically. 2008 proved to be a record year for data breaches, with the vast majority of these exposed records due to electronic data breaches. That news reinforces the importance of protecting personal information, and the fact that there are many steps that can be taken to protect data.

A DECADE AGO, WE WERE THE FIRST COMPANY TO ADDRESS SPYWARE THREATS AND ESTABLISHED AN ENTIRELY NEW COMPUTER SECURITY INDUSTRY

What challenges does Lavasoft face in the marketplace? What do you see as your advantages?

A decade ago, we were the first company to address spyware threats and established an entirely new computer security industry. The explosion of spyware in 2003 and the success of Lavasoft's Ad-Aware distribution triggered competitors to infiltrate in force. Today, there are many anti-spyware programs to choose from, and the anti-malware industry has become a multi-million dollar business.

What sets Lavasoft apart from all of the competition? We were the original anti-spyware company, and today, 10 years since our founding, we remain just as dedicated as ever to pioneering and providing innovative solutions to protect consumers and businesses from threats to their privacy.

Lavasoft continues to develop for safety, thoroughness, trust, and usability. We keep a pulse on the everyday computer user as well as the savvy IT admin to ensure that we develop for the masses. Our competitors are only worried about adding more bells and whistles to their products, which often results in products that are bloated and cumbersome. We develop products that allow every computer user to navigate like an expert through the complex maze of modern-day malware.

With our last release – Ad-Aware Anniversary Edition – we've focused our efforts on providing cutting-edge detection and removal, AND efficiency. The repair and clean-up of files after a malware infection is one of the main competitive advantages for Ad-Aware Anniversary Edition.

Most companies today are good at finding and removing malware, but there is a final step of repairing and cleaning-up the aftermath of a computer infection that distinguishes Ad-Aware from other products on the market.

Where do you see the current threats your products are guarding against in 5 years from now? What kind of evolution do you expect?

While it may not be easy to predict what we'll see in the next five years – threats change and proliferate on a daily basis – in general, the landscape is moving towards more blended threats, and of course, methods that enable cyber criminals to nab even larger profits.

The cyber crime industry will continue to evolve; it's already growing in sophistication and even mimicking real-world crime tactics. Malware writers are now stealthily blending threats – made up of different types of malicious software, combining traditional forms of spyware with traditional forms of viruses – in order to infiltrate PCs. In addition to that, as mobile devices become even more complex, and more software and services are developed for them, this will also create a broader, more exploitable platform to attack.

In short, consumers will not only need to be more vigilant about their security, they will need more versatile and advanced solutions in place to guard their privacy. Rest assured, Lavasoft will be ready.

AutoKrypt (www.net-security.org/software.php?id=726)

AutoKrypt is an encryption software designed for automation that will automatically encrypt or decrypt files and folders. AutoKrypt's encryption methods include password based, public and private key, secret key, OpenPGP password, OpenPGP public and private key.

MIMEDefang (www.net-security.org/software.php?id=214)

MIMEDefang is a flexible MIME email scanner designed to protect Windows clients from viruses. However, it can do many other kinds of mail processing, such as replacing parts of messages with URLs, adding boilerplate disclaimers, and so on. It can alter or delete various parts of a MIME message according to a very flexible configuration file. It can also bounce messages with unacceptable attachments.

SmartBackup (www.net-security.org/software.php?id=731)

No matter if you want to create full bootable backups or just set up a few important items for a small efficient network backup - If you are looking for a fast and straightforward solution, SmartBackup is perfect for you. Choose a local folder, your external HDD, network share or even WebDAV as your target and never lose your files again.

CryptoExpert 2008 Professional (www.net-security.org/software.php?id=305)

CryptoExpert 2008 Professional uses an on-the-fly encryption system to encrypt your files and keeps the data hidden in virtual drives. When you start the application and enter the password, it will mount the drives into Windows Explorer and you can access the content as if they were normal files; they are encrypted/decrypted automatically as they are requested by other applications.

Author: Scott Berkun | Pages: 408 | Publisher: O'Reilly | ISBN: 0596517718

It doesn't matter if you just got that promotion and you're supposed to oversee a project or if you're a one man band working on something, "Making Things Happen" is essentially for anyone.

Why is this review on a website dedicated to computer security? Well, project management is essential in every aspect of an organization and the security team is no exception. Having a firm grasp on how to work on a given task and create a positive environment filled with communication should be the basis for any project. This is where Scott Berkun comes in and delivers a book that shines a bright light into the right direction.

About the author

Scott Berkun worked on the Internet Explorer team at Microsoft from 1994-1999 and left the company in 2003 with the goal of writing enough books to fill a shelf. He makes a living writing, teaching and speaking.

Inside the book

What I really like about this book is the fact that it doesn't just tell you what to do. It guides you through the thinking process involved in the various stages of a projects and helps you evaluate what's important at every stage.

You've got the project going on as planned, the ideas are flowing and then something unfortunate happens. Things are bound to go wrong at a certain point and it's all about how you handle the situation that will decide the outcome of your project. Don't worry, the author has some advice for you, lots of it actually. That advice translates to the entire book as Berkun didn't just use his own experience but also interviewed more than a dozen project managers.

"Making Things Happen" is filled with examples you'll see as useful. For example, what's the difference between a good and a bad e-mail? The author provides both and illustrates the differences.

In order to make the material both easier to digest and find at a later time, each chapter closes with a summary of what's been presented as well as assorted exercises. I must say that this approach is exceptional as it not only makes you think about a variety of details and situations but it also sharpens what you've learned in the book, and forces you to apply it to real-world situations.

Final thoughts

Forget piles of unnecessary information, boring theories and charts, this title is all about real-world experience and practical examples. If your aim is to understand project management and discover how to manage your projects well, "Making Things Happen" is definitely the next book you should read.

Should Internet Service Providers (ISPs) supply their customers with an Internet connection over a network feed that is clean from illegal Web content and malware – programs that could cause network lag, compromise system security and threaten user privacy?

For example, a water company has to make sure that the water provided in their pipes is uncontaminated and flows securely all the way to their customers' water taps. Should that kind of extended "clean feed" responsibility be laid on the shoulders of ISPs – and, would that even be possible? Some ISPs are currently filtering certain illegal or "inappropriate" Web content. If the ISPs are already performing partial filtering, why omit the filtering of malware?

This article's objective is to explore ISP level malware filtering in order to see if malware can be neutralized at an early, preemptive stage – before it contaminates local networks and systems – and to investigate if any such projects are planned or ongoing.

The concept of clean feed

The concept of clean feed is based on the fact that Internet traffic is filtered with the help of a blacklist containing Internet addresses (URLs) of sites that are serving illegal Web content, such as content related to child pornography. A risk with this type of filtering approach is that whole domains could be blocked, rather than just the page serving the illegal content. This means that eventual false positives (blocking URLs serving legitimate content) could cause serious inconveniences for Internet users, especially if the filtering is done at the ISP level. In this perspective, the blocking of domains or IP addresses generates the same type of problems. In order to avoid such problems, the Internet traffic could be filtered dynamically, meaning that the traffic content is analyzed for certain words or images that are blocked if they match a certain signature that is stored in an image signature database.

The Swedish company, NetClean, has developed a clean feed solution that has been used for roughly two years by the Swedish ISP, TeliaSonera.

NetClean's WhiteBox solution uses a URL block list containing the addresses of sites that are to be blocked; these are sites serving illegal content related to child pornography. The URLs are resolved to their IP addresses by NetClean's WhiteBox server and those addresses are thereafter propagated to the networks in order to be filtered via BGP (Border Gateway Protocol, the core protocol for routing on the Internet). The network traffic is then routed and tunneled to the WhiteBox server that checks URL requests against the ones listed in the URL blocking list. When a match is found, a specific block-page is returned; otherwise the request is processed in normal manner, allowing the page to be accessed.

According to NetClean, the WhiteBox solution is not causing any network performance degradation. Blocking of unique URLs, such as www.domain.com/PageToBeBlocked, makes it possible to only block portions of websites. This supports the manual creation of blocking lists, such as blocking lists provided by the Australian Communications and Media Authority (ACMA) or the UK's Internet Watch Foundation (IWF). NetClean was the first company to develop a technique for detecting child pornography related images based on signatures; illegal images are given a unique ID signature, or digital fingerprint, with the help of image analysis software. This technique has been implemented in NetClean's Proactive package that also has been adopted by TeliaSonera, among others. The NetClean ProActive for Internet Content Adaptation Protocol (ICAP) works by routing network traffic through a proxy server. All pictures are then scanned and compared to the signatures in an image signature database before the request is made. Illegal images are blocked and the incidents are reported.

ISP level Web content filtering is already a reality in many countries, including Great Britain and Sweden.

ISP level Web content filtering

ISP level Web content filtering is already a reality in many countries, including Great Britain and Sweden.

In Australia, the Australian Communications and Media Authority (ACMA), recently ordered a second trial in order to evaluate ISP level content filters. The last similar trial was conducted in 2005. The fact that a "live pilot" of the Web content filtering solutions trial is ongoing makes the process even more interesting to follow; let's take a closer look at the report from the "Closed Environment Testing of ISP level Internet Content Filtering" trial that preceded the ongoing live pilot.

The main objective of the Australian trials was and is to find out if ISP-based filters could be used to provide a clean feed to Australian households. This was planned as a broad spectrum solution affecting all households that explicitly did not ask their ISPs to be exempted. The trials are meant to clarify how the filtering affects network performance along with the obvious – if and to what extent the filters can identify and block illegal and "inappropriate" Web content. What is considered inappropriate is not clearly defined in the report. The Australian Family Association, however, states, "Some content found online may not be illegal, but it is still of serious concern to many families, e.g., sites promoting suicide, or self-starvation or other forms of self-harm."

The ability to filter non-web traffic and the customizability of the filters are other factors that were and are investigated in the trials. ACMA uses its own blacklist for content that should be blocked. The ACMA blacklist consists of URLs associated to locations that serve images of sexually abused children and the blacklist is therefore considered, at this point, to merely be a child pornography blacklist. ACMA has also considered implementing more "sophisticated" filtering in order to provide extended web filtering services to Australian households that opt for it. Such "sophisticated" filtering could encompass automated content filtering, allowing for scanning and evaluation of text, images and video. This type of filtering is already used by Australia's New South Wales (NSW) public education sector, which filters Internet access for over a million computers across its networks.

The effects of filtering on performance and efficiency

According to the published ACMA trial report, the filtered network suffered from a performance degradation ranging from two to 87 percent between the tested filtering solutions. As a comparison, the previous test (conducted in 2005) showed a performance degradation ranging from 75 to 98 percent. The decrease of network lag between the two tests indicates a great improvement, but it is important to keep in mind that the filtering caused some degree of network lag; an extremely low level of network lag is crucial in large networks. According to the ACMA trial report, a network performance degradation of 2 percent, represented by the best performing filtering solution, is considered to be a standard or acceptable level among ISP level Web content filtering products.

The effectiveness of filtering solutions was tested using three separate lists of URLs, containing a total of nearly 4,000 URLs. The efficiency of blocking inappropriate web content ranged between 88 and 97 percent and the level of overblocking (blocking of legitimate content) varied in the range of one to eight percent between the tested filtering solutions.

Three of the tested filtering solutions managed to block more than 95 percent of the child pornography URLs on ACMA's blacklist, but none of the solutions offered 100 percent blockage. Even if three of the tested filtering solutions show extensive blocking capacity, the fact remains: some illegal content was not caught by the filters. Illegal content, such as child pornography, should not be able to pass efficient filtering solutions and the fault tolerance, in this case, should be zero.

The filtering of malware

There are many different Unified Threat Management (UTM) systems on the market. Network-based UTM appliances are often offered with bundles including Web content filtering, anti-spam, anti-virus, and network load balancing services for both small home or office networks and larger enterprise-level networks. This seems to also be the case with ISP level filtering products; the latest ACMA Web content filtering solutions trial report states that many of the filtering solutions represented in their test could be extended with anti-virus, anti-spam and anti-malware capabilities.

In the UTM appliance market, high customizability is considered important because "one-size-fits-all" solutions often fail to fully address the needs posed by highly diversified network environments. Vendors, such as Websense and BlueCoat Systems, provide high capacity standalone Web content filtering solutions that can be extended to also offer malware filtering. Such extended solutions usually depend on the usage of security gateways or proxy servers that are set to scan and filter the traffic between Internet and local networks. When looking at the NetClean example, the Swedish company that detects child pornography-related images based on signatures, they also rely on routing network traffic through a proxy server (which supports ICAP) where images can be matched against an image signature database.

NetClean has developed a technological partnership with BlueCoat Systems, experts in high-end caching systems and secure proxy solutions. The NetClean ProActive for ICAP is verified to work with BlueCoat's Proxy SG appliances and with proxy servers such as SafeSquid, Squid, Mara Systems and Webwasher. NetClean states that they, in conjunction with BlueCoat Systems and their ProxySG appliances, can deliver "complete security solutions", including virus-scanning, even for large ISPs.

So, if the technology exists – and apparently it does – why is it not implemented in large scale by ISPs in order to provide an extended clean feed, including malware filtering, to their customers?

Could it be the fact that such filtering solutions have not yet matured to a level where the network performance degradation, caused by extended traffic filtering, could be held down to an acceptable level? However, the latest ACMA Web content filtering solutions trial showed that the best performing filtering solution caused a 2 percent network performance degradation, which was regarded as acceptable. ACMA also seems open to extended filtering solutions for customers that opt for it.

The fact that some illegal Web content manages to slip through the filter, along with the fact that illegal and inappropriate Web content carried by other protocols than HTTP is not filtered, raises the question of the usability of the potential filtering solution. Also, the Australian government seems to focus on filtering what they regard as "inappropriate" content, even if some Australian ISPs, like Internode, would rather focus on malware filtering because such filtering would generate more value.

The fact is that non-web traffic, in general, and peer-to-peer traffic, in particular, constitutes a great portion of the total Internet traffic. Efficient Web content filtering solutions should therefore also be able to filter and block content that is carried by non-web protocols, such as via Simple Mail Transfer Protocol (SMTP) or Real Time Streaming Protocol (RTSP). The latest ACMA trial showed that two Web content filtering solutions were able to block "inappropriate" content that was carried via SMTP and that only one solution could block "inappropriate" content in streaming media.

In order to filter network data streams for malware in an efficient manner, several protocols – such as Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), Internet Message Access Protocol (IMAP), and peer-to-peer protocols (P2P) – need to be filtered.

In addition to this, Common Internet File System (CIFS), Secure Sockets Layer (SSL), MAPI, SOCKS, AOL IM, Yahoo IM, Microsoft IM, RTSP, QuickTime and TCP-Tunneling needs to be filtered when aiming for a complete content filtering solution.

ISP level malware filtering could be implemented by tunneling all network traffic through transparent Proxy servers where the traffic is filtered. Anti-virus or anti-spyware solutions based on ICAP could be used to scan both incoming and outgoing content in real time. Malicious content is blocked while legitimate content passes through unaltered.

Passing files could be hashed – creating full or partial digital signatures of the files – and matched against the signatures stored in a malware signature database. Another approach would be to cache files in order to subject them to a heuristic scan, performed later within the file cache. If a file within the file cache is found to be malicious by the heuristic scan, it's signature is inserted in the malware signature database so that it may be blocked in the future.

Malware URLs could be saved in a database for blocking or research purposes. Spyware creators often recompile their spyware code in order to avoid detection by malware scanners that use signature-based (such as the md5 value of files) scanning. The recompilation can be done in an automated manner creating large numbers of unique binaries; we often see this type of behavior among certain rogue software. Using URL filtering can be a usable alternative in such cases, but block-lists must be updated continuously and the websites or IPs listed have to be checked and rated continuously in order to keep the block-lists accurate.

In order to filter network data streams for malware in an efficient manner, several protocols need to be filtered.

Concluding thoughts

The aim of this article was to clarify the eventual possibilities for ISP level malware filtering and to illuminate if such solutions are implemented or planned. Clean feed Web content filtering solutions are implemented in certain countries, like Sweden, the UK, and Australia. In these cases, the clean feed is focused on filtering Web content related to child pornography. ISPs are thus filtering the network feed, but only to a certain extent; they omit the filtering of viruses and malware. Yet, the technology for such filtering is available. ACMA states in their Web content filtering solutions trial that many of the tested solutions could be extended to also provide anti-virus and anti-malware protection.

ICAP compatible anti-virus or anti-malware scanners, installed on transparent proxies, could be used for real-time scanning of tunneled network traffic.

What is the reasoning behind only offering clean feed in its current extent? Spyware, malware, worms and viruses pose a serious threat to both system integrity and user privacy. The prevalence of such malicious programs could also threaten the stability of critical systems and networks. Some ISPs, such Australia's Internode, would like to focus on malware filtering rather than performing questionable filtering on "inappropriate" Web content – filtering that could be argued to represent a form of Internet censorship.

At the same time, most ISPs acknowledge that it is important to protect systems against the pests that are present in their network feed, but the protective means are to be taken by individuals through the use of proper anti-virus and anti-spyware software. Many ISPs worldwide sell separate anti-virus and anti-spyware software bundles to their customers as optional extras, instead of providing a malware-free network feed. Providing malware filtering as an extension of the existing clean feed could prove to be a competitive advantage for ISPs that offer such solutions to their customers.

In the publication "Making the Internet Safe", the Australian Family Association states, "In contrast the community wants primary filtering to be done at the ISP level." If that statement is true, it raises an important final question: where does the responsibility of the ISP start and where does it end?

Pekka Andelin is a Malware Researcher at Lavasoft (www.lavasoft.com).

The impact of the consumerization of IT on IT security management

by Alexei Lesnykh

Driven by the proliferation of high-end consumer technology such as PDAs, MP3 players and smartphones, we have seen increasing adoption of consumer technology in the corporate environment. The age of consumerization of IT, defined as the blurring of lines between corporate IT and consumer technology, is well and truly upon us. Thanks to the fundamental growth of endpoint device capabilities and the corresponding changes in security threat profiles, this new era has significant ramifications for the management and enforcement of corporate IT.

Consumerization goes mobile

Today's personal mobile devices (smartphones and PDAs) have already been proven to increase personal and employee productivity. Despite a rather limited range of mobile applications and services being used in typical corporate environments – mostly email, IM and, less frequently, Presence Awareness – the use of smartphones is becoming increasingly commonplace in mid to large sized organizations.

According to a survey from TechTarget more than 25% of the corporate workforce used employee-supplied mobile devices in 2008. Recent technology advancements including the chip makers' continued confirmation of the full validity of Moore's Law, suggest that IT consumerization is only going to become more widespread. The world is entering an age of ubiquitous mobile broadband connectivity: a global proliferation of Wi-Fi; the fast-growing commercial deployment of 3G/HSPA networks; and the "injection" of Mobile WiMAX by Intel's fifth-generation processor platform, Montevina, which promises to enable WiMAX for 750 million people by 2010. With the new generation of SoC platforms, ignited by Intel's invasion of the mobile SoC market, and the subsequent explosive growth of enterprise-class mobile applications, the world is going ultra mobile.

The consumobilized threat

The consumerization of corporate IT will soon mobilize the entire corporate workforce, with everyone using either company-supplied or individually-owned mobile devices or MIDs.

The Yankee Group predicts that this will lead to Zen-like co-operative IT management models being deployed to maximize employees' productivity.

From an IT security perspective, the task of managing 'rogue' or disgruntled employees in a consumobilized enterprise will become a real art – especially as a high degree of co-operative behavior and self-discipline will be expected and required from all employees including those who are discontented, malicious, negligent, or forgetful. In this way, the very same technology advancements and social trends that drive the progress of consumerization will also cause a sharp increase in information security risks for the enterprise, based on the development of 'production quality' mobile malware, and – to an even larger extent - the growth of corporate data leakage from and through employees' mobile devices. The typical size of a mobile device's removable flash memory (currently 4 - 8GB) is already sufficient for storing and running a standard Operating System. The significant increase in mobile internet devices (MIDs) computing ability, together with a tenfold drop in their power consumption, has already triggered rapid mobile OS and application industry growth, making the development of 'commercial' mobile malware extremely profitable. From its current stage of proof-of-concept prototypes, this mobile malware will very quickly move to a "production-quality" stage, thus increasing the probability of attacks to mobile devices and their infection.

How soon this happens really depends on how quick and dedicated the mobile OS vendors will be in their efforts to control this emerging market. Although, realistically, it is unlikely that we will see any impact before the end of 2009 because the 'target market' for commercial malware needs to be mature enough to justify investment in their 'product' development.

Conversely, the threat of corporate data leakage through personal mobile devices is unavoidable and immediate. Unavoidable because certain features of human nature will not change: since there is no ultimate cure for accidental errors, negligence or malicious intent, mobile devices will continue to be lost and stolen. Immediate because nothing new is required for exercising the threat and it is happening right now.

Mobile encryption is not enough

Every instance of data leakage through a mobile device is a two-step process: firstly, uncontrolled data transfer from a corporate server/host-based resource to the device and, secondly, further unauthorized transfer of this data from the device to the outside. To mitigate this efficiently, existing Data Leakage Prevention (DLP) solutions for mobile devices include two layers of defense. Firstly, DLP components residing at servers, PCs or dedicated network appliances prevent data leaking from the corporate resources to the mobile devices by intercepting and filtering data in all communications channels used by those devices. Secondly, device-resident infosecurity components should prevent data from uncontrollably leaking from the mobile devices.

Reviewing the functions of security components running on mobile devices, it appears that there is currently only one truly effective mechanism that directly prevents data leakage – the device-resident encryption. Typically implemented as 'file/volume encryption' or 'whole device encryption', it blocks access to encrypted files and other objects stored in the memory of stolen or lost devices, as well as removable memory cards.

Security vendors also tout remote data wiping as an additional mechanism for preventing data leakage from missing mobile devices. However, realistically, this should not be considered as a reliable means of protection as any cyber thief will immediately remove the memory card of the stolen device for analysis on a 'failproof' device.

All other device-resident security components – FW, VPN, device/port control, anti-virus/anti-malware, IDS, application control, NAC, user/device authentication – are not designed for informational data and type filtering and, therefore, cannot be used to determine whether outbound traffic contains any leak to block. As for anti-spam device components, they work in the opposite direction, filtering data coming in rather than preventing the downloading of unsolicited data to the device.

Although cryptographic solutions like "whole device encryption" could completely eliminate data leakage from stolen or lost mobile devices, they are not a DLP panacea for mobile devices. This is because applications use data in RAM rather in plain, decrypted form; so nothing prevents users from deliberately or accidentally sending plain data to an external destination from within an opened network application like email, web-browser, or instant messaging (IM). As a result, a negligent employee could forward an email with order delivery instructions to a subcontractor without noticing that the attachment to the email contains clients' personal data that should not be revealed to third parties.

The only way to achieve truly encryption-based protection against mobile data leaks would be in a physically isolated intranet-type system without any external communications at all. However, this scenario is useless to any business or public sector organization as their operations are inherently based on external communications.

According to Deloitte & Touche and the Ponemon Institute about 45 per cent of US businesses do not use encryption to protect their data. However, in the consumerized corporate future, because of employees' privacy concerns, the percentage of personal mobile devices without protection by employer-supplied encryption solutions is likely to be much higher.

Without underestimating encryption as the most effective security technology for preventing data leakage from mobile devices today, it should be acknowledged that once the data gets to the device there is, and always will be, a high risk of it being uncontrollably leaked to the outside. This is why, for the foreseeable future, a critically important layer of corporate defense against mobile data leaks needs to be the intelligent control over data delivery channels to the mobile device.

Gone with the sync

Mobile devices can basically import data through three channel types: network applications, removable memory cards, and local connections to PCs. Today, there are numerous products and solutions on the market for preventing data leakage to mobile devices through network applications such as email, web-browsing, file transfer, web-mail and instant messaging.

Implemented as server-side components or dedicated network appliances that use well-developed data and file type filtering as well as content-based filtering technologies, these solutions have proven to be highly effective for fighting data leaks and ensuring users' compliance with applicable security-related legislation and industry standards.

These data filtering technologies have already been integrated with several host-based endpoint device/port control products available today, so the data uploaded from PCs to removable memory cards is intercepted and filtered to block detected leaks.

Importantly, these DLP solutions are based on underlying protocol parsing techniques for the most popular network applications, and intercepting file system calls from some office applications.

However, the synchronization of local data between mobile devices and PCs is implemented by very specific applications that do not use network application protocols, and do not interact with office applications. Technically speaking, this means that no existing file type detection or content-based filtering solution can control data flow through local connections from PCs to mobile devices and the only possible method of preventing data leakage through local sync currently is to completely prohibit it at device or local port-type level on the concerned PC.

This means that any company concerned with uncontrolled data leakage though mobile devices should prohibit their employees from synchronizing data between corporate PCs and mobile devices. This is obviously unacceptable, even today, since it would completely block the use of mobile devices in the business. The problem is that if local syncs are allowed – as is the case in most organizations today – then every click on a "Sync" button means that highly valued corporate data may be potentially transferred to a personal mobile device without any way of controlling or tracing it.

Weakly protected local sync communications already constitute a serious security issue for organizations. In the future, as consumerization progresses, this issue could grow into a major security problem and business risk. This is why developing a comprehensive DLP solution for local sync connections of mobile devices needs to be urgently addressed by the infosecurity industry.

Developing the solution

So what should the security industry be doing to address the mobile security threats brought about by IT consumerization? The key part of the architecture for preventing data leakage needs to be local sync parsing. The local sync data leakage prevention architecture should be built as a stack of integrated security mechanisms including bottom-up endpoint device/port control, local sync application parsing, file type filtering, and content-based filtering technologies. In addition, a central policy-based management console integrated with a major systems management platform, comprehensive centralized logging, reporting and evidence enablement components need to be put in place.

Every layer of the architecture controls those parameters of a local connection it is designed to deal with by blocking or filtering prohibited elements out, and detecting and marking the types of objects to be controlled by a higher-layer architecture component to which the classified data flow is then passed for further processing.

The device/port control component of the architecture is responsible for detecting and controlling the presence of a locally connected mobile device, the type of connection interface or port type, device type and ideally the device model and its unique ID. The output can then be passed to the local sync parsing component, which parses the sync traffic, detects its objects (e.g. files, pictures, calendars, emails, tasks, notes, etc.) filters out those prohibited, and passes allowed data up to the file type filter. The file type filtering component checks the input flow, deletes those files not allowed, and filters information data to detect and block the pieces of human-understandable data failing to comply with the corporate security policy.

Sync parsing is the most important “piece of cake” to develop because the rest of the required enforcement components are already available on the market just in implementations designed not for the local sync. Not only is local sync parsing key, but its scale (i.e. the range of supported mobile OS platforms) and implementation quality will also be critical for its market adoption. With local sync parsing in place, the other components can be stepwise integrated in the stack by adjusting the existing ones.

Examining the local sync DPL solutions commercially available on the market, the situation is quickly improving with Microsoft ActiveSync and Windows Mobile Device Center (WDMC) protocol filtering now available. Security administrators can now centrally and granularly define which types of data users are allowed to synchronize between corporate PCs and their mobile personal devices, including files, pictures, calendars, emails, tasks, notes, and other ActiveSync and WDMC protocol objects.

Administrators can also centrally block or allow the installation and execution of applications on corporate mobile devices. In addition, it is now possible to detect the presence of mobile devices regardless of which local port or interface it is connected to.

The security threat brought about by the consumerization of IT and the consequent mobilization of the workforce is real and upon us. Organizations need to take immediate steps to ensure that they address this threat before it gets out of control and the infosecurity market needs to continue to develop solutions to mitigate the unavoidable risk brought about by the growth of consumer technology in the corporate environment.

Alexei Lesnykh is the Business Development Manager at DeviceLock (www.devicelock.com).

2nd DIGITAL SECURITY FORUM

www.digitalsecurityforum.eu

26-27 JUN LISBON 2009

Hotel Ollissipo Oriente

The Digital Security Forum aims to be a reference in European security conferences and training events, allowing for infosec professionals to network and acquire knowledge, by discovering the industry`s best practices, new methodologies, technologies and tools.

Keynote Speakers

Prof. Howard Schmidt
CISSP, CISM - President & CEO of Information Security Forum, International President of ISSA

Dr. Louis Marinos
Senior Expert on Risk Management, ENISA

Adam Laurie
Director of "THE BUNKER", and developer of RFIDiot.org

Patricia Peck
Lawyer/Digital Law Expert

Workshops

Christian Bockermann
ModSecurity

This list is not final, and only includes the already confirmed participants

Registration

Open on January 2009

Pricing

Before 31st January: **€200**
From 1st February to 28th February: **€240**
From 1st March on: **€360**
All prices include VAT at 20%.

Call for Papers Deadline

The deadline for papers / proposals submission is the 10th of February 2009, and should be sent to:
cfp@digitalsecurityforum.eu

www.catodesign.com

Sponsors

pontosi

Partners

diplomatatours
um sorriso de ida e volta

CATO DESIGN

Media Partners

Turismo de Lisboa

InfoSec ONline.pt

Virtually Informed - Security News

(IN)SECURE insecuremag.com